Avaya Video Conferencing Manager Deployment Guide

August 2011

Avaya Video Conferencing Manager

This guide is for network administrators who use Avaya Video Conferencing Manager to manage video and voice communications systems in an IP environment.

Installing	Describes the installation and initial configuration process. This section also describes how to upgrade and uninstall Avaya Video Conferencing Manager.	Installing and Configuring Avaya Video Conferencing Manager
Managing	Describes routine device, infrastructure, and user management tasks.	Managing Devices, Infrastructure, and User Accounts
Scheduling	Describes events, including scheduling calls and other device events.	Scheduling Events
Reporting	Describes how to generate reports in data or graphical formats.	Generating Reports
Administering	Describes how to use Avaya Video Conferencing Manager Administrator to change configuration settings in Avaya Video Conferencing Manager.	Administering Avaya Video Conferencing Manager
Reference	Lists permissions and alarms.	User Role Access Alarms by Category
Troubleshooting	Describes symptoms, possible causes, and potential solutions to issues you may encounter after installing or upgrading Avaya Video Conferencing Manager.	Troubleshooting

Related documentation is available from support.avaya.com.

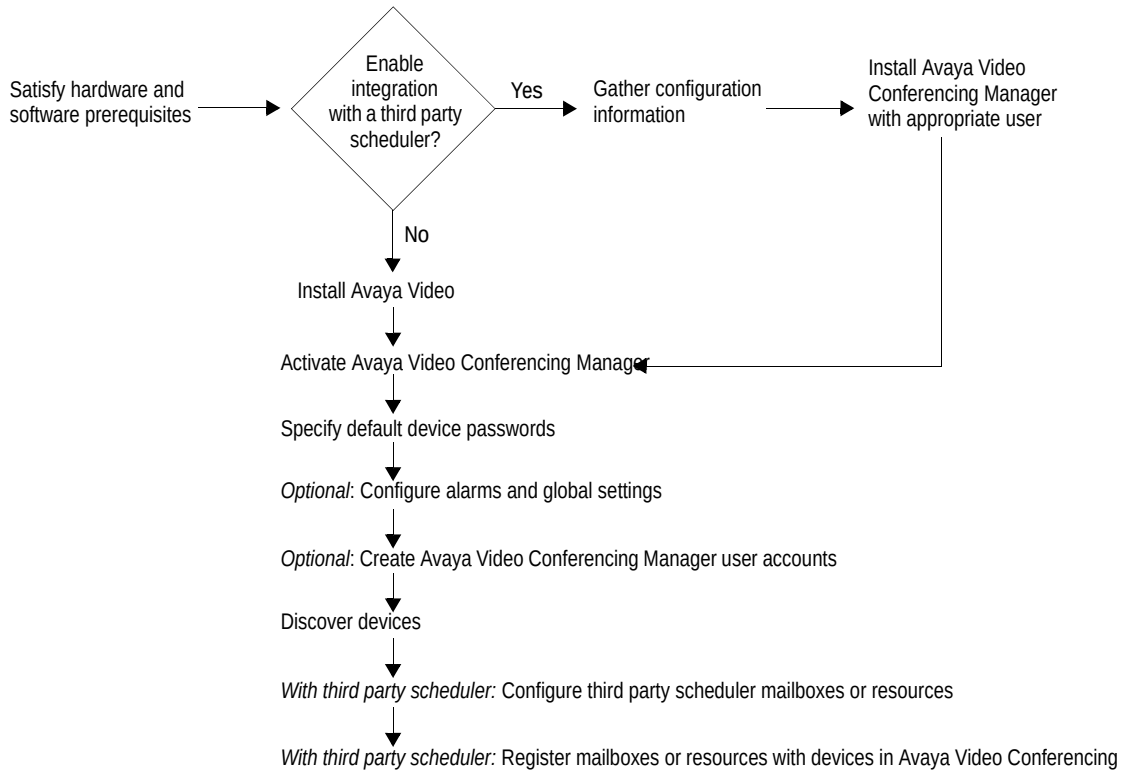
Section 1: Installing and Configuring Avaya Video Conferencing Manager

This section includes the following topics:

- Preparing for a Avaya Video Conferencing Manager Deployment
- Hardware and Software Prerequisites
- Installing Avaya Video Conferencing Manager
- Upgrading Avaya Video Conferencing Manager
- Configuring Your Environment
- Uninstalling Avaya Video Conferencing Manager
- Integrating a Third Party Scheduler

Preparing for a Avaya Video Conferencing Manager Deployment

The following diagram shows the tasks for deploying Avaya Video Conferencing Manager for the first time:


Satisfy hardware and software prerequisites
Enable integration with a third party scheduler?
Yes
Gather configuration information
Install Avaya Video Conferencing Manager with appropriate user
No
Install Avaya Video
Activate Avaya Video Conferencing Manager
Specify default device passwords
Optional: Configure alarms and global settings
Optional: Create Avaya Video Conferencing Manager user accounts
Discover devices
With third party scheduler: Configure third party scheduler mailboxes or resources
With third party scheduler: Register mailboxes or resources with devices in Avaya Video Conferencing

Avaya recommends a phased approach to deploying Avaya Video Conferencing Manager that includes planning, installing, testing, and training before going live.

Prerequisites	Ensure that your environment meets the hardware and software prerequisites, including port access and client support requirements in Hardware and Software Prerequisites.
Third Party Scheduling Applications	By integrating one of the following third party scheduling applications with Avaya Video Conferencing Manager you can schedule calls in Avaya Video Conferencing Manager without a user account: • Microsoft Exchange Server 2003: requires Microsoft Active Directory • Microsoft Exchange Server 2007 with SP1: requires Active Directory • Microsoft Exchange Server 2010 with SP1: requires Active Directory • Google Apps Gmail and Google Calendar: Premier Edition users only; requires Microsoft Active Directory Application Mode (ADAM) CAUTION: You cannot change the user authentication method or the third party scheduling application that you choose to integrate after installing Avaya Video Conferencing Manager. To change other integration settings after installing Avaya Video Conferencing Manager, refer to Mail Integration Settings. Read more at Integrating Microsoft Exchange Server with Avaya Video Conferencing Manager and Integrating Google Apps Gmail and Google Calendar with Avaya Video Conferencing Manager.
Device Usernames and Passwords	When the application attempts to manage a device, it logs in to the device's command line or administrative interface using the login information that you supply. Before you discover devices, gather login information for the devices that you intend to manage. Read more at Specifying Default Passwords for Device Management.
Users	Avaya Video Conferencing Manager supports multiple users and controls their access to functionality with roles. Review the information about user roles and accounts in Managing User Accounts to determine which users to add and roles to assign. User Role Access identifies the access level by role for each task that users can perform. Administrators can also create custom user roles. Read more at Role Management Settings.
Alarms	Alarms alert users to events and conditions that may require user intervention. Before training users to monitor and respond to alarms, determine which alarms you wish to monitor. Read more at Alarms by Category and Alarms Configuration. You can also forward traps from all managed devices to third party monitoring systems or on a device-specific basis. Read more at Northbound Settings.
Global Settings	With Avaya Video Conferencing Manager Administrator you can set configuration options and enable or disable integration with a third party scheduling application. Read more at Administering Avaya Video Conferencing Manager. Avaya recommends that you configure these settings before training users. Avaya Video Conferencing Manager uses the Microsoft ADAM server settings that you provide during installation to set LDAP settings and populate the corporate directory on managed Avaya, LG, and LifeSize video systems. By default, managed systems and external devices appear in the directory. You can create and set a default hierarchy of managed devices to appear on the directory screen of these systems when a user browses the corporate directory hierarchically. Read more at Managing Device Groups.
Test Environment	Avaya recommends that you create a test environment before deploying Avaya Video Conferencing Manager. To create a test plan, use the device management and call scheduling procedures in Managing Devices, Infrastructure, and User Accounts and Scheduling Events.

Training	Use the procedures in this guide to develop training for the Avaya Video Conferencing Manager features you plan to use in your environment.
Reports	Determine which reports you want to generate and their frequency. Avaya Video Conferencing Manager includes a reports subscription feature that automates report generation and delivery. Read more at Generating Reports.
Maintenance	Avaya recommends that you back up your installation. Read more at Database Management. If you plan to integrate Microsoft Exchange Server, review Maintenance with Microsoft Exchange Server Integration.

Hardware and Software Prerequisites

Ensure that your environment meets the requirements in the following sections. If you are upgrading from a previous release, refer to Upgrading Avaya Video Conferencing Manager for important information about upgrade prerequisites.

Hardware

The minimum server configuration depends on the number of devices that Avaya Video Conferencing Manager manages.

Number of Managed Devices	Processor	RAM	Hard Disk Space
Fewer than 100	2.5 GHz dual core	2 GB	35 GB
100 or greater	2.5 GHz dual core	4 GB	35 GB

NOTE Dual NIC cards are not supported on the Avaya Video Conferencing Manager server.

Software

Depending on your operating system, you must install and activate the following Windows components or roles on the server. Avaya Video Conferencing Manager uses ADAM or Active Directory Lightweight Directory Service (AD LDS) to populate settings and the corporate directory on managed Avaya systems and, optionally, for user authentication.

NOTE The installation program quits and an error appears if ADAM or AD LDS is not on the server.

Operating System	Components or Roles	Directory Service
Microsoft Windows Server 2003 Standard edition with SP1 (minimum) or SP2 (recommended) 32- or 64-bit (x86/x64 only)	Components: • Application Server Console • ASP.NET • Enable Network COM+ Access • Enable Network DTC Access • Internet Information Server (IIS) v6.0 or later	Microsoft ADAM
Microsoft Windows Server 2008 R2 Standard edition (64-bit) (x64 only)	Server Roles: • AD LDS • Web Server (IIS) Role Services: IIS Management Compatibility	Microsoft AD LDS

Additional software requirements:

- If you intend to use SSL to access Avaya Video Conferencing Manager from a web client, ensure that you obtain a valid server certificate.
- Ensure that Active Directory is not installed on the server on which you intend to install Avaya Video Conferencing Manager and that the server is not a domain controller.
- The Avaya Video Conferencing Manager installation program installs the Microsoft .NET Framework 2.0, if not already installed, and PostgreSQL v8.3. Before you run the installation program, consider the following:
  - You have administrator rights to install the applications.
  - An existing PostgreSQL installation does not exist.
  - OpenSSL version.

    If OpenSSL exists on the server, ensure that the version is 0.9.7 or later or delete the LIBEAY32.dll and SSLEAY32.dll files (located in the `C:\windows\system32` folder). The Avaya Video Conferencing Manager installation program installs a compatible version of these files if OpenSSL does not exist on the server.

If the Avaya Video Conferencing Manager installer detects an earlier version, you must delete the LIBEAY32.dll and SSLEAY32.dll files and uninstall Avaya Video Conferencing Manager before running the Avaya Video Conferencing Manager installation program again. Read more at Uninstalling Avaya Video Conferencing Manager.

CAUTION If you are performing an upgrade and the Avaya Video Conferencing Manager installation program encounters an incompatible version of OpenSSL, you cannot continue the upgrade or return your existing Avaya Video Conferencing Manager installation to its previous state without uninstalling Avaya Video Conferencing Manager, reinstalling the previous version, and restoring its database from a backup.

- Avaya recommends that you use a static IP address for the machine on which Avaya Video Conferencing Manager is installed.

Client Support

The computer you use to access the Avaya Video Conferencing Manager user interface must have 256 MB memory and Adobe Flash Player.

NOTE Adobe Flash Player is included with the Avaya Video Conferencing Manager installation program as an optional installation step, or you can download it directly from adobe.com.

Ports

Application Management

Application	Ports	Description
IIS to Avaya	TCP port 8085	Avaya Video Conferencing Manager is based on Microsoft's .NET Framework and uses this port for IIS to Avaya server communication.
ADAM and AD LDS	TCP port 389	By default, used by ADAM and AD LDS. You cannot change this port setting. Ensure that any firewalls that are installed on the Avaya Video Conferencing Manager server are configured to allow incoming traffic on this port.
Scheduling with Radvision and LifeSize MCUs	TCP port 3336	Avaya Video Conferencing Manager uses this port when scheduling conferences through Radvision and LifeSize MCUs.
User interface	TCP and UDP port 80	The user interface is hosted on IIS on port 80.
	TCP port 443	Used for the SSL option.
	TCP port 4296	Used for dynamic updates.
Adobe Flash security	TCP port 843	Avaya Video Conferencing Manager requires TCP port 843 for Adobe Flash security. Adobe Flash clients retrieve a master policy file from this port on the server.

Device Management

Avaya Video Conferencing Manager supports device management through the following standard APIs. Communication with these devices is through default ports provided for FTP, SNMP, and HTTP.

Protocol	Ports	Description
FTP	TCP port 21	Outbound communication from Avaya Video Conferencing Manager to Codian, Tandberg, and Polycom devices.
Telnet	TCP port 23	Outbound communication from Avaya Video Conferencing Manager to Tandberg devices.
	TCP port 24	Outbound communication from Avaya Video Conferencing Manager to Polycom devices.
SSH	TCP port 22	Outbound communication from Avaya Video Conferencing Manager.
SNMP v1, v3	UDP port 161	Inbound communication: Avaya Video Conferencing Manager connects to this port on a device to retrieve data from the device.
	UDP port 162	Avaya Video Conferencing Manager listens on this port to receive traps from a device. When the device needs to forward a trap, it connects to the Avaya Video Conferencing Manager server on this port to deliver the trap.
HTTP	TCP and UDP port 80	
LDAP	TCP port 389	ADAM or AD LDS for inbound communication from Avaya devices to the Avaya Video Conferencing Manager server.

LifeSize Transit Management

If Avaya Video Conferencing Manager (installed in the LAN) manages LifeSize Transit Server and video systems that are outside of the LAN, ensure that you open the following ports on the firewall:

SSH	Avaya Video Conferencing Manager manages LifeSize devices through TCP port 22.
HTTP HTTPS	Avaya Video Conferencing Manager manages LifeSize Transit Server through TCP and UDP port 80 and TCP port 443.
SNMP	Required for Avaya Video Conferencing Manager to receive traps for video devices.

NOTE Avaya Video Conferencing Manager requires ICMP to ping LifeSize Transit Server and video devices.

Data Storage

Avaya Video Conferencing Manager stores data in the PostgreSQL database management system. The installation program installs PostgreSQL on the same server as Avaya Video Conferencing Manager.

A database instance is created using Trusted Windows Authentication. The connection mechanism uses the PostgreSQL Data Provider. Avaya Video Conferencing Manager uses an LDAP-based H.350 compliant address book.

Installing Avaya Video Conferencing Manager

NOTE For upgrade instructions, refer to Upgrading Avaya Video Conferencing Manager.

Installing Avaya Video Conferencing Manager includes the following tasks:

- Install Microsoft Windows components (Windows Server 2003) or roles (Windows Server 2008 R2).
- Install either Microsoft ADAM (on Microsoft Server 2003) or Microsoft AD LDS (on Microsoft Server 2008 R2).
- Run the Avaya Video Conferencing Manager installer.

The Avaya Video Conferencing Manager installation program also installs Avaya Video Conferencing Manager Administrator, a web-based tool for managing Avaya Video Conferencing Manager. Refer to Administering Avaya Video Conferencing Manager.

Installing Components on Microsoft Windows Server 2003

1. From the Windows **Control Panel**, choose **Add or Remove Programs** and click **Add/Remove Windows Components** in the left panel.
2. From the **Windows Components Wizard**, select **Application Server** and click **Details**.
3. Enable the following required subcomponents:

Application Server Console	Provides a central location from which to administer web applications.
ASP.NET	Required to deploy ASP.NET web applications to a production server. Avaya Video Conferencing Manager is an ASP.NET web application.
Enable Network COM+ Access	Builds on Component Object Model (COM) integrated services and features. Most Avaya Video Conferencing Manager components are service components.
Enable Network DTC Access	Coordinates COM+ transactions. Avaya Video Conferencing Manager components use DTC for remote calls.
Internet Information Server (IIS)	Provides the infrastructure for .NET and existing web applications and services. The default enabled subcomponents **Internet Information Service Manager** and **World Wide Web Service** are required to run Avaya Video Conferencing Manager.

4. Click **OK**.
5. Click **Next** to complete the installation.
6. Close the **Add or Remove Programs** window.

Installing Server Roles on Microsoft Windows Server 2008 R2

1. On the **Start** menu, point to **Programs**, **Administrative Tools**, and then click **Server Manager**.
2. In **Roles Summary**, click **Add Roles**.
3. In the **Before you Begin** page, click **Next**.
4. In the **Server Roles** page, select the following:
   - **Active Directory Lightweight Directory Services**
   - **Web Server (IIS)**
5. Click **Next**.
6. Click **Next**.
7. Click **Install**.

Installing Role Services on Microsoft Windows Server 2008 R2

1. On the **Start** menu, point to **Programs**, **Administrative Tools**, and then click **Server Manager**.
2. In the navigation pane, expand **Roles**, right-click **Web Server (IIS)**, and then click **Add Role Services**.
3. In the **Select Role Services** pane, scroll down and select **IIS 6 Management Compatibility**. Ensure that this selection is expanded and that all of its service components are also selected.
4. In tFhe **Select Role Services** pane, click **Next**.
5. In the **Confirm Installation Selections** pane, click **Install**.
6. Click **Close** to exit the **Add Role Services** wizard.

Installing Microsoft ADAM or AD LDS

Before installing Avaya Video Conferencing Manager, ensure that the appropriate directory service is installed on the server that you intend to use for Avaya Video Conferencing Manager

Microsoft Windows Server 2003 uses Microsoft ADAM with SP1. Download ADAM SP1 for Microsoft Windows Server 2003 from the Microsoft Download Center.

Microsoft Windows Server 2008 R2 uses Microsoft AD LDS. Installing AD LDS for use with Avaya Video Conferencing Manager includes adding the role **Active Directory Lightweight Directory Services**. Refer to Installing Server Roles on Microsoft Windows Server 2008 R2.

The Avaya Video Conferencing Manager installer creates an instance named `AvayaVideoConfMgradaminstance`. The installer uses the ADAM user that you specify for logging in to Avaya Video Conferencing Manager as the administrator of the ADAM or AD LDS instance.

Installing Avaya Video Conferencing Manager Software

Avaya recommends that you collect the following required information before installing:

- Fully qualified domain name of your organization’s SMTP server.
- Email address of the person who will receive Avaya Video Conferencing Manager alarms.
- IP address for the ADAM server.
- Domain suffix of the ADAM directory tree structure (for example, *example.com*).
- If enabling Microsoft Exchange Server integration:
  - IP address or fully qualified domain name of the Microsoft Exchange Server.
  - Domain name for the Microsoft Exchange server.
  - Avaya Video Conferencing Manager email address and password described in task 1 in Microsoft Exchange Server Integration Overview.
- If enabling Google Apps Gmail and Google Calendar integration, the email address and password of the Google Apps user that you created for Avaya Video Conferencing Manager in Prerequisites.
- IP address for the Avaya Video Conferencing Manager server.

Running the Avaya Video Conferencing Manager Installer

NOTE To avoid installation errors, disable security software (including Windows Firewall) before running the Avaya Video Conferencing Manager installer. After installation, you may re-enable the security software.

Insert the distribution media and follow the prompts. If the **Welcome** screen does not appear, double-click **setup.exe** from the Avaya Video Conferencing Manager CD.

Use the following configuration tables for information about specific settings.

Avaya Video Conferencing Manager Configuration

SMTP Server	Enter the fully qualified domain name of the SMTP server for your organization. This server is used for sending alert emails. This value is required for alerts.
To Email Address	Enter the email address of the recipient who will receive alerts. This value is required for alerts.
From Email Address	Enter the email address that will appear as the *From* address of an alert message (for example, *AVCM@example.com*).
Use https	Enabled by default. Specify whether to use SSL for communication between the Avaya Video Conferencing Manager server and the web clients or to use HTTP. NOTE: If you intend to manage LifeSize Desktop, select this option or enable it manually after installation on IIS on the server. To learn how to set up an HTTPS service in IIS, refer to `http://support.microsoft.com/kb/324069`.
Make Avaya Video Conferencing Manager the default web site?	Choose **Yes** for the server's hostname to be an alias for the Avaya Video Conferencing Manager URL. Users can enter this hostname in their browsers to access Avaya Video Conferencing Manager. For example: `http://<hostname>`

Avaya Video Conferencing Manager Server - LDAP Configuration

ADAM Settings	From the **ADAM Server IP** list, select the IP address for the ADAM server. NOTE: You cannot modify **Port**.
	Enter the domain suffix for the ADAM directory tree structure. For example: *example.com*.
User Authentication	Select and enter values for one of the following user authentication methods. You cannot change user authentication methods after installing the application. • **Configure for ADAM**. Required for Google Apps Gmail and Google Calendar. Create a user account for logging in to Avaya Video Conferencing Manager. Enter a username and password. -OR- • **Configure for Active Directory**. Required for Microsoft Exchange Server; the Active Directory server must be the same one used by your Exchange Server. Specify an existing domain and an existing user account for logging in to Avaya Video Conferencing Manager. The specified user must be configured so that passwords never expire. Avaya Video Conferencing Manager uses Active Directory to access the user accounts for authentication purposes only, and does not add, delete, or modify user accounts. The machine on which you are installing Avaya Video Conferencing Manager must already be on the domain if you choose this option. The user you define in this step must have administrator privileges; and the password is case-sensitive. Because this user can edit and delete all user accounts, ensure that you store the login credentials in a safe place.

Depending on the user authentication method you chose, a configuration dialog box appears for Google Calendar or Microsoft Exchange.

- **Configuration for Google Calendar support** (Microsoft ADAM). By default, **Enable Google Calendar Integration** is selected. You can clear this checkbox and enable integration in Avaya Video Conferencing Manager Administrator after the installation completes. Optionally, you can enter the following information:

Avaya Video Conferencing Manager email address	Enter the email address of the Google Apps user that you created for Avaya Video Conferencing Manager in Prerequisites.
Avaya Video Conferencing Manager email password	Enter the password for the Google Apps user that you created for Avaya Video Conferencing Manager.

- **Avaya Video Conferencing Manager configuration for Microsoft Exchange support** (Active Directory). By default, **Enable Exchange server integration with Avaya Video Conferencing Manager** is selected. You can clear this checkbox and enable integration in Avaya Video Conferencing Manager Administrator after the installation completes. Optionally, you can enter the following information:

Exchange server requires HTTPS access	Select this checkbox if your Microsoft Exchange Server requires HTTPS access.
• **Exchange 2003** • **Exchange 2007/ Exchange 2010**	Specify which version of Microsoft Exchange Server you wish to integrate with Avaya Video Conferencing Manager.
Exchange Server address	Enter the Microsoft Exchange Server's IP address. NOTE: If your Microsoft Exchange Server environment utilizes a Front End (FE) server or a Client Access Server (CAS), enter the IP address of the FE or CAS instead.
Domain Name	Enter the domain name for the Microsoft Exchange Server.
Avaya Video Conferencing Manager email address	Enter an email address. For example: *AVCM@example.com*. This is the email account Avaya Video Conferencing Manager monitors to provide scheduling integration with Microsoft Exchange Server. Set the size of this mailbox to 500 MB. Log in to the account in Microsoft Outlook at least once to make it available for Avaya Video Conferencing Manager. While logged in, ensure the email box is set to the correct time zone. Avaya recommends that you set the archive interval for the Avaya Video Conferencing Manager mailbox to one week to prevent this mailbox from exceeding its storage limit. CAUTION: This email box must be dedicated for use by Avaya Video Conferencing Manager. Do not send general email to it or use it to send email. You must not open this email box or modify any email messages in it. Doing so will interfere with the integration of Microsoft Outlook scheduling with Avaya Video Conferencing Manager scheduling.
Avaya Video Conferencing Manager password	Enter a password for the Avaya Video Conferencing Manager email box.

NOTE Restart your computer to ensure that the changes take effect. If the installation fails, refer to Troubleshooting.

Upgrading Avaya Video Conferencing Manager

The Avaya Video Conferencing Manager installation program installs the Microsoft .NET Framework 2.0 if not already installed. During an upgrade, the Avaya Video Conferencing Manager installer changes the ASP.NET version of all web sites installed in IIS to v2.0. Other web sites installed in IIS that are not running in their own application pools may not function properly after the upgrade. To work around this issue after performing the upgrade, refer to Troubleshooting.

Upgrade Prerequisites

Before you upgrade your Avaya Video Conferencing Manager installation, complete the following tasks:

- Avaya recommends that you back up your Avaya Video Conferencing Manager database before performing an upgrade. Refer to the product documentation for the version of Avaya Video Conferencing Manager from which you are upgrading for backup instructions.
- Create a backup copy of the SharedXML folder and the `*.config` files that are located in the installation folder.
- Install Microsoft ADAM or AD LDS. Read more at Installing Microsoft ADAM or AD LDS.
- Ensure that the server on which Avaya Video Conferencing Manager is installed has at least 35 GB of free disk space.
- Ensure that the server on which Avaya Video Conferencing Manager is installed does not have an Active Directory installation and is not a domain controller.
- Ensure that you have administrator rights to perform the upgrade.
- Ensure that Avaya Video Conferencing Manager is not in use during the upgrade.
- If OpenSSL exists on the server, ensure that the version is 0.9.7 or later. Read more at OpenSSL version.

Performing an Upgrade

1. Ensure that you complete all tasks in Upgrade Prerequisites.
2. On the Avaya Video Conferencing Manager CD, double-click **setup.exe**. The program automatically detects an existing Avaya Video Conferencing Manager installation that is eligible for an upgrade.
3. When prompted to continue with the upgrade, click **Next**.
4. Click **Finish**.
5. Restart the server.

NOTE If the installation that you upgraded used OpenLDAP for authenticating users in Avaya Video Conferencing Manager, the upgrade changes each user's password to `avaya` when it migrates data from OpenLDAP to ADAM or AD LDS. You can change the passwords for these users on the **User Management** page. Refer to Modifying a User Account.

Configuring Your Environment

After installing Avaya Video Conferencing Manager, configure your environment by completing the following tasks:

- Accessing Avaya Video Conferencing Manager.
- Obtaining the License Key.
- Specifying Default Passwords for Device Management.
- Discovering Devices.
- Familiarizing yourself with the Avaya Video Conferencing Manager Dashboard.
- Integrating a Third Party Scheduler.

Accessing Avaya Video Conferencing Manager

After installing Avaya Video Conferencing Manager on a server, you can access the user interface by entering the URL in a supported web browser:

```
http://<hostname>
```

If Avaya Video Conferencing Manager is not configured to be the default web site for the server, you must enter the full path for Avaya Video Conferencing Manager. For example:

```
http://<hostname>/avaya
```

Troubleshoot login issues as follows:

Incompatible version of Adobe Flash Player	If Avaya Video Conferencing Manager detects an incompatible version of Adobe Flash Player or Adobe Flash Player is not installed on your system, a page appears with a link to installation files for a supported version.
Launch page does not appear	Refer to Troubleshooting.
Username and password	These values were defined when you installed the application and set up User Authentication for the LDAP configuration.
Cookies	Enable cookies for Avaya Video Conferencing Manager to remember the username and password for subsequent sessions if you select **Remember me**.

After logging in as a user with administrator privileges, you can set up other users. Refer to Managing User Accounts.

Obtaining the License Key

To use Avaya Video Conferencing Manager, you must configure the software with a license key (on the Avaya Video Conferencing Manager CD) and activate the software. Contact Avaya Technical Services if you do not have a license key and need assistance.

NOTE After you activate the license key, you cannot reuse the key.

1. Access Avaya Video Conferencing Manager.
2. On the navigation bar, click .
3. In the **License key** section, enter the license key included with the Avaya Video Conferencing Manager CD.
4. Click **Save**.

   Avaya Video Conferencing Manager automatically unlocks the software.

Specifying Default Passwords for Device Management

When Avaya Video Conferencing Manager attempts to manage devices, it uses the device login information that you specify in the **Password** page for each make of third party devices. If you do not specify a valid username and password for third party devices, or if the password that you specify has been changed on a device, **Login failed** appears in the **Status** column for the devices and you cannot manage them until you update the password for each device in Avaya Video Conferencing Manager.

Using Avaya Video Conferencing Manager to update a password for a device changes the password in the Avaya Video Conferencing Manager database. It does not change the password stored on the device. To use Avaya Video Conferencing Manager to change the password stored on the device, the device must be managed in Avaya Video Conferencing Manager. The password is automatically updated in the Avaya Video Conferencing Manager database as well. Read more at Managing Device Passwords.

Credentials for Discovering Devices

Follow these steps to enter default usernames and passwords for discovering devices:

1. Access Avaya Video Conferencing Manager.
2. On the navigation bar, click .
3. In the **Other Protocols** section, select the make of the third party device for which you wish to enter a username and password. Avaya Video Conferencing Manager supports only one username and password for each make of supported device as the default to use during device discovery.
4. Click **Add**.

Community Strings

By default Avaya Video Conferencing Manager uses SNMP to show detailed information about a discovered device, such as its make, model, and software version. The community string is a password used to access the device when you are sending SNMP traps. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device discards the request and does not respond. The default value of the community string is `public`. To change the default value, follow these steps:

1. On the navigation bar, click .
2. In the section that pertains to the SNMP version that you use on your network, select the make of the third party device.
3. Enter a value for **Community String** for SNMP v1 or v2, or enter a **Username** for SNMP v3 or other protocols.
4. Click **Add** (SNMP v1 or v2) or **Add User** (SNMP v3).

Discovering Devices

After you configure default passwords for device management, follow these steps to discover and begin managing devices in Avaya Video Conferencing Manager:

1. Access Avaya Video Conferencing Manager.
2. On the navigation bar, click .
3. In **Actions**, click **Discover devices** and then click **Submit**.
4. Discover a single device or discover devices in a range of IP addresses.
   - To discover a single device, choose **Single IP** in **Search By**. Enter the IP address in the **IP Address** box.
   - To discover devices in a range of IP addresses, choose **IP Range** in **Search By**. Enter the IP address range in the **From** and **To** boxes.

   NOTE A large range of IP addresses may cause a delay due to network latency. You can continue to interact with the Avaya Video Conferencing Manager interface during this process. For best results, limit the range to a maximum of 255.

5. **Start managing once discovered**, the default, enables Avaya Video Conferencing Manager to attempt to log in to and maintain communication with a device after discovering it. This option also enables you to manage the device through Avaya Video Conferencing Manager. Consider clearing this checkbox if you have fewer licenses in Avaya Video Conferencing Manager than devices on your network; or you do not wish to manage certain devices in Avaya Video Conferencing Manager.

6. Click **Start Discovery**.

NOTE Avaya Video Conferencing Manager automatically discovers instances of LifeSize Networker as gateways.

Discovering Devices Registered to a Gatekeeper

Avaya Video Conferencing Manager automatically discovers gatekeepers, but not the devices registered to them. If a gatekeeper appears on the **Devices** page after you discover devices, complete the following steps to discover the devices registered to the gatekeeper:

1. On the **Devices** page, locate each entry for a discovered gatekeeper.
2. Click the entry, click , and then click **Discover registered devices**.

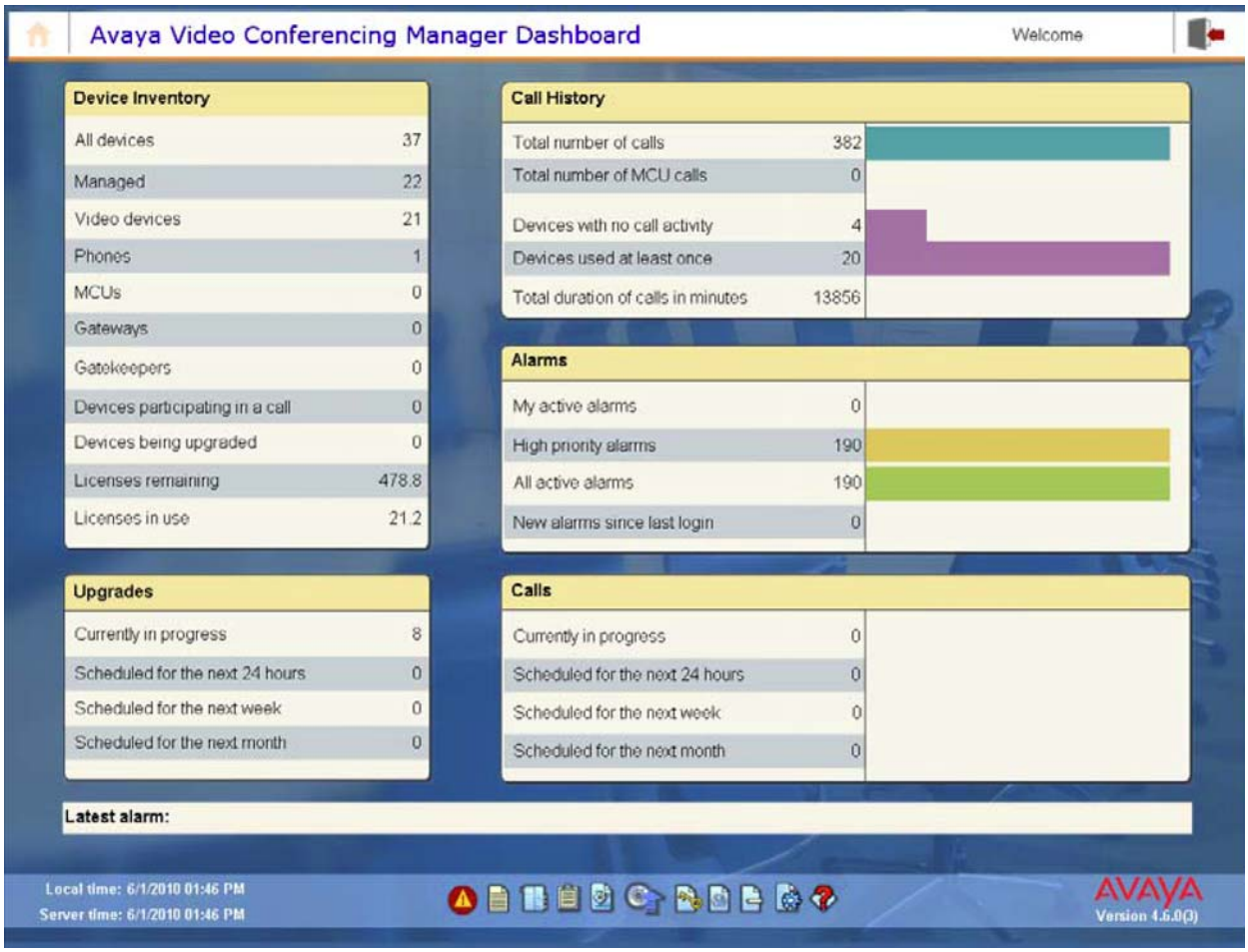
   The status of the discovery appears at the bottom of the page and the device list refreshes automatically.

Managing LifeSize Gatekeeper with Avaya Video Conferencing Manager

1. On the computer on which LifeSize Gatekeeper is installed, open the Windows **Services** window.
2. Right-click **SNMP service** and click **Properties**.
3. Click the **Security** tab.
4. Select **Accept SNMP packets from any host**, or add the IP address of the Avaya Video Conferencing Manager server in **Accept SNMP packets from these hosts**.
5. If the value of **Community** in the **Accepted community names** dialog box is not **public**, note the value that appears and do the following:
   a. In Avaya Video Conferencing Manager, access the **Passwords** page.
   b. In the **SNMP v1/SNMP v2** section of the page, click **Avaya** for **Make name**.
   c. In **Community string** enter the value that you noted at the beginning of this step.
   d. Click **Add**.

Avaya Video Conferencing Manager Dashboard

As shown in the following example, the Avaya Video Conferencing Manager Dashboard provides a comprehensive view of your systems and their status.



Click any row in the following sections of the dashboard to obtain more detailed information or perform management tasks:

- **Device Inventory**. Lists the number of known devices and the total number of licenses purchased and in use.
- **Upgrades**. Lists scheduled and in-progress device upgrades.
- **Call History**. Lists call history and statistics at a glance.
- **Alarms**. Lists current alarms and alarm history.
- **Calls**. Lists current and scheduled calls.

Click to return to the Avaya Video Conferencing Manager Dashboard from any screen and to log off from Avaya Video Conferencing Manager.

The navigation bar at the bottom of the screen provides access to the following features and functionality:

View and manage alarms.

Discover and manage devices in the network.

View, manage, and schedule calls, template actions, device offline schedules, and upgrades.

Generate a variety of periodic reports, inventories, summaries, and diagnostics.

Create templates for devices, and back up and restore devices.

Upload upgrade packages to Avaya Video Conferencing Manager.

Specify default passwords for devices and protocols.

Add or import, delete, or modify Active Directory or Microsoft ADAM users.

Activate Avaya Video Conferencing Manager software.

Perform a system audit to view all actions performed in Avaya Video Conferencing Manager:

- by logged in users
- automatically by the Avaya Video Conferencing Manager server
- on a managed device

Manage LifeSize Desktop installations.

Open Avaya Video Conferencing Manager Administrator (available to administrators only).

Access user help.

Only those icons associated with features to which the logged in user has access appear on the navigation bar. For more information about user accounts, refer to Managing User Accounts.

Uninstalling Avaya Video Conferencing Manager

The Avaya Video Conferencing Manager uninstall program removes all components that Avaya Video Conferencing Manager installed, except the installation directory, any log files and device upgrade files that are stored in the installation directory, and the Avaya_PostgreSQL directory (which is at the same level as the Avaya directory). You must remove these directories manually after uninstalling Avaya Video Conferencing Manager.

NOTE This release of Avaya Video Conferencing Manager does not appear in the **Add or Remove Programs** window.

To uninstall Avaya Video Conferencing Manager from the server, follow these steps:

1. Access **Start->All Programs->Avaya->Video Conferencing Manager->Uninstall**.
2. When prompted to remove Avaya Video Conferencing Manager, click **Yes**.
3. When prompted to remove PostgreSQL, select **Remove** and click **Yes**.
4. On the **Start** menu, click **Run** and enter `inetmgr`.
5. Expand the tree to show the **Default Web Site** node.
6. Remove `AvayaVideoConferencingManager`.
7. In the **Default Web Site** directory, remove `AvayaAura.aspx`.
8. Right-click the **Default Web Site** node, and then click **Properties**.
9. Click the **Documents** tab and remove `Avaya.aspx` from the list of files.
10. Restart your computer.

Integrating a Third Party Scheduler

Integrating a third party scheduler allows users to schedule calls in Avaya Video Conferencing Manager without having a Avaya Video Conferencing Manager user account. Without this feature, users of video and voice communications systems typically must call a help desk or similar scheduling facility to schedule a call through Avaya Video Conferencing Manager.

Integrating Microsoft Exchange Server with Avaya Video Conferencing Manager

Integrating Microsoft Exchange Server with Avaya Video Conferencing Manager includes the following features:

- Users can schedule calls in Avaya Video Conferencing Manager through Microsoft Outlook.
- Avaya Video Conferencing Manager administrators can use email commands to manage video communications devices. Refer to Managing a Device Through Email.
- Human participants in video calls scheduled in Avaya Video Conferencing Manager through Microsoft Outlook can specify an external video system. Refer to Specifying a Preferred Method of Participation.

Prerequisites

Ensure that you have reviewed and completed tasks in the following sections before integration:

- Preparing for a Avaya Video Conferencing Manager Deployment

> NOTE Install the Microsoft Exchange Server version listed in Third Party Scheduling Applications or in the release notes for Avaya Video Conferencing Manager.

- Hardware and Software Prerequisites
- Installing Avaya Video Conferencing Manager
- Configuring Your Environment

Microsoft Exchange Server Integration Overview

Task 1: Create an email account in Microsoft Exchange Server for Avaya Video Conferencing Manager

Avaya Video Conferencing Manager monitors this email account to provide scheduling integration with Microsoft Exchange Server and Microsoft Outlook. Read more at Avaya Video Conferencing Manager email address.

Task 2: Configure Avaya Video Conferencing Manager for Active Directory

When the Avaya Video Conferencing Manager installer prompts you to choose a mechanism for authenticating Avaya Video Conferencing Manager users, enter values for **Configure for Active Directory**. Ensure that the Active Directory server that you specify is the same one used by your Microsoft Exchange Server.

Task 3: Enable and configure integration during installation (optional)

You can enable and configure integration during or after installation. If you accept the default to enable integration with Microsoft Exchange Server during installation, supply the following information:

- If Microsoft Exchange Server requires HTTPS, select the corresponding checkbox.
- The version of Microsoft Exchange Server that you wish to integrate with Avaya Video Conferencing Manager.
- Microsoft Exchange Server hostname or IP address.
- Domain name for the server.
- Avaya Video Conferencing Manager email address and password from task 1.

If you enable and configure integration after the installation completes, select configuration options in Avaya Video Conferencing Manager Administrator. Read more at Microsoft Exchange Server Settings.

Task 4: Choose a deployment option

Option 1: Create a resource mailbox for each conference room

Benefits	Limitations
With this option, Microsoft Outlook users do not need to add the video or voice devices to the meeting request as separate invitees. Avaya Video Conferencing Manager automatically places the scheduled call to the devices that reside in the conference rooms that the meeting organizer includes in the meeting request. Consider using this option if conference rooms are dedicated for use as video or voice conferencing rooms.	Users may not want to use video or voice devices in the meetings. Users who wish to add an MCU or a video recorder to a call must remember to invite the device as a separate invitee.

- **Video and voice communications systems**. Create a resource mailbox in Microsoft Exchange Server for each conference room that contains a video or voice system managed by Avaya Video Conferencing Manager. Forward each conference room mailbox to the Avaya Video Conferencing Manager mailbox. In Avaya Video Conferencing Manager, associate the managed system with the email address of the mailbox resource for the conference room. When Microsoft Outlook users add conference rooms to a meeting request, Avaya Video Conferencing Manager automatically schedules the system associated with these conference rooms and places the call at the scheduled meeting time.
- **MCUs, on demand conferences, and video recorders**. Configure mailbox resources in the same way as described in Option 2: Create a resource mailbox for each device.

Option 2: Create a resource mailbox for each device

Benefits	Limitations
Microsoft Outlook users can create meeting requests with or without voice or video devices as invitees.	Microsoft Outlook users must include both the conference room and the video or voice device as invitees to schedule calls.

- **Video and voice communications systems**. Create a resource mailbox in Microsoft Exchange Server for each video or voice system managed by Avaya Video Conferencing Manager. Forward each mailbox to the Avaya Video Conferencing Manager mailbox. In Avaya Video Conferencing Manager, associate the managed video or voice system with the email address of the mailbox resource. When Microsoft Outlook users create meeting requests, they add the conference rooms and the systems located in each room as separate invitees.
- **MCUs**. Create a resource mailbox in Microsoft Exchange Server for each managed MCU (including LifeSize Bridge). Forward each MCU mailbox to the Avaya Video Conferencing Manager mailbox, and associate the MCU with the email address of the mailbox resource for the MCU.
- **On demand conferences**. Create a resource mailbox in Microsoft Exchange Server for each on demand conference. Forward the mailbox to the Avaya Video Conferencing Manager mailbox, and associate the on demand conference with the email address of the mailbox resource. You must also register the on demand conference with a LifeSize Bridge. Read more at On Demand Conferences in LifeSize Bridge.
- **Video conference recorders**. To allow meeting participants to select a managed video recorder in a call scheduled through Microsoft Outlook, **create only one mailbox resource for all managed video recorders**. Do not associate the email address of this mailbox resource with any device managed in Avaya Video Conferencing Manager. Instead, Avaya Video Conferencing Manager automatically selects the video conference recorder to use in the call if the meeting organizer invites this resource. Enter the recorder resource's email address in Recorder Email on the **Mail Integration Settings** page in Avaya Video Conferencing Manager Administrator and assign recorder affinity to a video and voice communications device in Avaya Video Conferencing Manager.

Creating Mailbox Resources in Microsoft Exchange Server

When you create mailbox resources in Microsoft Exchange and register your managed systems with those mailboxes, Microsoft Outlook users can schedule those devices as required participants or locations in meeting requests. Those scheduled meetings then appear as scheduled calls within Avaya Video Conferencing Manager on the **Events** page. Calls scheduled through Avaya Video Conferencing Manager also appear as meetings in Microsoft Outlook, thus preventing double booking.

When you schedule an upgrade, a template comparison, or take a communications system offline in Avaya Video Conferencing Manager, the event is shared with Microsoft Outlook and the device becomes unavailable for scheduling other events.

Before you create mailbox resources, consider the following:

- If you selected Option 1: Create a resource mailbox for each conference room and you already have room mailboxes in Microsoft Exchange for scheduling purposes, begin with step 7 (Exchange Server 2003) or step 6 (Exchange Server 2007/2010).
- To allow meeting participants to add an MCU to a meeting scheduled through Microsoft Outlook, begin with step 1 to create a mailbox resource for each MCU.
- To allow meeting participants to add a video recorder to a call, start with step 1, but **create only one mailbox resource for all video conference recorders**.

Microsoft Exchange Server 2003

If you are using Microsoft Exchange Server 2007 or 2010, refer to Microsoft Exchange Server 2007 and 2010.

Complete the following steps to create mailbox resources:

1. Navigate to **Programs->Microsoft Exchange->Active Directory Users and Computers**.
2. Create a new user. Right-click the directory icon containing the Active Directory users and select **New Object->User**.
3. Enter the **Full name** and **User logon name** and click **Next**.
4. Enter and confirm the user's password, select **Password never expires**, and click **Next**.
5. Select **Create an Exchange mailbox** and enter an **Alias**, **Server**, and **Mailbox Store**. Click **Next**.
6. Click **Finish**.
7. Configure forwarding of the messages sent to this mailbox to include Avaya Video Conferencing Manager's listener mailbox.
   a. Right-click the user you created in step 2 and select **Properties**.
   b. Click the **Exchange General** tab of the **Properties** dialog box.
   c. Enter the **Mailbox store**.
   d. Click **Delivery Options** and select **Forward to** from the **Forwarding address** section.
   e. Click **Modify**.
   f. In the **Enter the object name to select** box, enter the mailbox you created for Avaya Video Conferencing Manager during installation and click **OK**.
   g. Select **Deliver message to both forwarding address and mailbox** and click **OK**.
8. To configure a mailbox to associate with a managed video or voice device, register the mailbox for **Auto Accept Agent** to automatically process meeting requests. For more information, refer to the Registering Mailboxes section of the Microsoft TechNet web site:

   ```
   http://technet.microsoft.com/en-us/library/bb124104(EXCHG.65).aspx
   ```

   To configure a mailbox for an MCU or for the video recorder, **do not** configure the mailbox for **Auto Accept Agent**.

9. Register the mailbox with the corresponding voice or video communications system in Avaya Video Conferencing Manager. Refer to Registering Mailboxes with Devices in Avaya Video Conferencing Manager.

NOTE It may take up to five minutes for the new user to be active and available after you create it.

Microsoft Exchange Server 2007 and 2010

If you are using Microsoft Exchange Server 2003, refer to Microsoft Exchange Server 2003.

Complete the following steps to create mailbox resources:

1. Start the Microsoft Exchange Management Console.
2. Create a mailbox for the conference room that houses your video system. Under **Recipient Configuration**, right-click the **Mailbox** icon and select **New Mailbox**.
3. Select **Room Mailbox** for mailbox type and click **Next**.

NOTE Select **Room Mailbox** even if you are creating a mailbox for a device, including an MCU, as described in Option 2 in Microsoft Exchange Server Integration Overview.

4. Create a new user or select a current user if the conference room in which you have your audio and video communications system already has a user in Active Directory.
5. Enter an alias for the user and select the appropriate Mailbox database. Click **Next**. The mailbox and the corresponding user are created.
6. To set up forwarding to Avaya Video Conferencing Manager's listener mailbox, double-click the mailbox created in step 5 and select the **Mail Flow Settings** tab. Double-click **Delivery Options**.
7. Select **Forward To** and **Deliver message to both forwarding address and mailbox** and click **Browse**. Select the mailbox you created for Avaya Video Conferencing Manager during installation and click **Finish**.
8. To enable the user so that you can associate it with a video communications system, start the Active Directory User Management Console.
9. Locate the user you created in step 5. Right-click and select **Enable**.
10. Right-click and select **Reset Password**.
11. Enter and confirm the password and select **Password never expires**.
12. If you are creating a mailbox for an MCU, skip to step 16.

13. In Microsoft Outlook Web Access, log in to the email account for the video system and click **Options** in the upper right corner of the window.

    NOTE You must perform this step in Microsoft Outlook Web Access with Internet Explorer.

14. In the **Options** menu, click **Resource Settings** and do one of the following:
    - To configure a mailbox for a video or voice system, select **Automatically process meeting requests and cancellations**.
    - To configure a mailbox for a video recorder, ensure that **Automatically process meeting requests and cancellations** is not selected.
15. Click **Save**.
16. Register the mailbox with the corresponding voice and video system in Avaya Video Conferencing Manager. Refer to Registering Mailboxes with Devices in Avaya Video Conferencing Manager.

    NOTE It may take up to five minutes for the new user to be active and available after you create it.

Integrating Google Apps Gmail and Google Calendar with Avaya Video Conferencing Manager

Integrating Google Apps with Avaya Video Conferencing Manager allows users to schedule calls in Avaya Video Conferencing Manager without having a Avaya Video Conferencing Manager account.

Prerequisites

Ensure that you have reviewed and completed tasks in the following sections before integration:

- Preparing for a Avaya Video Conferencing Manager Deployment
- Hardware and Software Prerequisites
- Installing Avaya Video Conferencing Manager
- Configuring Your Environment

Additionally, complete the following tasks:

- Set up a Google Apps Premier Edition account. Refer to the Google Apps web site.
- Log in to your Google Apps control panel. On the Dashboard, ensure that the Email and Calendar services are active. Refer to the documentation for Google Apps if these services are not active.

- Create a user in Google Apps for Avaya Video Conferencing Manager. Refer to the Google Apps Admin Help for creating a new user. Avaya recommends that you give this user a first and last name and a username that clearly identifies it as the Avaya Video Conferencing Manager user. Make note of the username and email address of this user. You will need this information if you choose to configure Google Calendar integration settings when you install Avaya Video Conferencing Manager or if you choose to configure these settings in Avaya Video Conferencing Manager Administrator after installing Avaya Video Conferencing Manager.

NOTE Avaya Video Conferencing Manager does not support single sign on in Google Apps.

Configuring Google Apps for Use with Avaya Video Conferencing Manager

1. Ensure that you have a calendar resource to associate with each video or voice communications device, MCU, and on demand conference for scheduling with Google Apps Calender.

   You can use an existing conference room resource for devices that reside in the conference room or create a new resource for each device. Because MCUs reside on the network rather than in a conference room, ensure that you have a calendar resource for each MCU. For more information about these deployment options, refer to Hardware and Software Prerequisites. To create a resource in Google Apps Calendar, refer to the Google Apps Admin Help.

   Video recorders only: **create only one resource for all recorders**. Avaya recommends that you name this resource to clearly identify it as a generic video conference recorder resource, such as Record Me or Record this Conference.

   Copy and paste each resource's email address to a separate document and note the managed device in Avaya Video Conferencing Manager you wish to associate with each resource email address.

2. As the Avaya Video Conferencing Manager user in Google Apps, complete the following steps to subscribe to each resource's calendar:

   a. In Google Apps, log in to the email account of the Avaya Video Conferencing Manager user.

   b. Log in to the calendar account for the Avaya Video Conferencing Manager user.

   NOTE You may be prompted to set the time zone if this is the first time this user has logged in.

   c. In the **Other calendars** section, click the **Add** link. A menu of options appears.

   d. Click **Add a coworker's calendar**.

   e. In **Contact Email**, enter the email address of the resource that you wish to associate with a managed video or voice communications device or MCU in Avaya Video Conferencing Manager. For example:

   ```
   example.com_343434333838373939343 9@resource.calendar.google.com
   ```

   f. Click **Add**. The resource's name appears in **My calendars**.

g. Configure notifications for the resource calendar that you added in the previous step. In **My calendars**, click the down arrow next to the name of the other calendar. In the menu of options that appears, click **Notifications**. The notifications details screen for that calendar appears.

h. Select the following options in the **Email** column:

- **New invitations**
- **Changed invitations**
- **Canceled invitations**
- **Invitation replies**

i. Click **Save**.

j. Repeat steps c through i for each remaining resource.

3. If you created a resource for video recorders and subscribed to its calendar in the previous step, configure calendar settings for this resource calendar to automatically add all events regardless of conflicts. In **My calendars**, click the down arrow next to the name of the other calendar for the video conference recorder resource and then click **Calendar settings**. On the **Calendar Details** tab in the **Auto-accept invitations** section, select **Automatically add all invitations to this calendar**.
4. In Avaya Video Conferencing Manager, click to configure mail integration settings in Avaya Video Conferencing Manager Administrator. Refer to Google Apps Settings.
5. Register the calendar resources in Avaya Video Conferencing Manager. Refer to Registering Mailboxes with Devices in Avaya Video Conferencing Manager and Registering a Mailbox with an On Demand Conference.

Registering Mailboxes with Devices in Avaya Video Conferencing Manager

NOTE Use this procedure to register a mailbox with LifeSize Bridge.

1. In Avaya Video Conferencing Manager, click on the navigation bar to access the **Devices** page.
2. Use the **Browse** window to list all managed devices.
3. Locate the device you wish to associate with the mailbox or calendar resource that you created in Microsoft Exchange or Google Apps.
4. Click in the **Tools** column. The **Register with mailbox** dialog box appears.

NOTE If this icon does not appear, click and ensure that **Register with mailbox** is selected in the **Tools** section.

5. Enter the mailbox you created for the device and click **Register**.

NOTE *Video recorders only*: Do not associate the email address of the mailbox resource that you created for recorders to an individual managed recorder. Instead, ensure that you entered the email address of the recorder mailbox resource on the **Mail Integration Settings** page in Avaya Video Conferencing Manager Administrator and assigned recorder affinity to video communications devices in Avaya Video Conferencing Manager.

Refer to Microsoft Exchange Server Settings or Google Apps Settings and Recorder Affinity.

Avaya Video Conferencing Manager confirms successful registration by changing the yellow envelope icon from to and by writing a confirmation message to the **Status** box below the list of devices.

Registering a Mailbox with an On Demand Conference

1. In Avaya Video Conferencing Manager, click on the navigation bar to access the **Devices** page.
2. In **Actions**, select **On demand conferences** and click **Submit**.
3. Select the on demand conference entry and click in the **Tools** column.

   The **Register with mailbox** dialog box appears.
4. Enter the mailbox or calendar resource you created for the on demand conference and click **Register**.

   The yellow envelope icon changes from to .

NOTE With affinity set on an on demand conference to a LifeSize Bridge, you can register a mailbox also through the LifeSize Bridge device. Read more at Managing On Demand Conferences for a LifeSize Bridge.

Troubleshooting Mail Registration Failures in Microsoft Exchange Server

If the mailbox registration fails, Avaya Video Conferencing Manager writes an error message to the **Status** box below the list of devices. Some of the possible reasons for failure include:

- Mail forwarding from the device mailbox to the Avaya Video Conferencing Manager mailbox you set up during installation is not in effect. Ensure that the mailbox resource for the device in Microsoft Exchange Server is set up to forward its messages to the Avaya Video Conferencing Manager mailbox. Also ensure that automatic processing of meeting invitations and cancellations is enabled.
- Avaya Video Conferencing Manager cannot contact the Microsoft Exchange Server.
- The Microsoft Exchange Server authentication credentials entered during the installation of Avaya Video Conferencing Manager are incorrect. Authentication credentials include: domain name, username and password of the Avaya Video Conferencing Manager mailbox, and whether HTTPS access is required.
- The mailbox is already registered to another managed device.

NOTE To unregister the mailbox address from the **Register with mailbox** dialog box, click **Unregister**.

Section 2: Managing Devices, Infrastructure, and User Accounts

This section describes routine management tasks.

Devices	Click to manage devices and device groups. Click to manage LifeSize Desktop.	Managing Devices Managing Device Groups
Alarms	Click to view and manage alarms.	Managing Device Alarms
Templates	Click to manage templates. Apply a template to a single device or multiple devices simultaneously.	Using Templates to Configure Devices
Maintaining	Learn how to upgrade device software; manage license keys; and back up and restore device configurations.	Maintaining Devices
Infrastructure	Click to manage infrastructure devices and provisioning from the **Devices** page.	Managing User Accounts
Users	Click to manage user accounts.	Managing User Accounts

Managing Devices

This section describes device management tasks.

Navigation	Device Status Device Tools Browsing Devices Refreshing Device Information
Overview	Device Management Overview Device Details
Management tasks	Managing External Devices Managing Device Passwords Sending a Message to a Device MCU Affinity Recorder Affinity Setting a Default Service Prefix for an MCU Forwarding SNMP Traps with Northbound Settings Managing a Device Through Email

Click on the navigation bar or click any device category in **Device Inventory** on the **Dashboard** to access the **Devices** page. By default, the following information appears for each device:

Status	Status of the managed device. Additional status information appears at the bottom of the page when you perform an action on the page. Read more at Device Status.
System Name	You can edit the system name of a managed device by double-clicking this field in the entry for a device and entering a new value. You can enter only the following characters in the this field: A-Z a-z 0-9 ~ ! @ # $ % ^ & * ( ) _ - + = { } | \ < , > . ? / ; : \
Make	Indicates the device brand name. Example: LifeSize, Polycom, or Tandberg.
Model	Defines the device model name. Example: Team 220.
Device Type	Shows a pictorial representation of the device type. If the type is unknown, appears.
Tools	Device-specific tools. Read more at Device Tools.

Click to select additional columns of information or hide tools that appear on the **Devices** page. You cannot hide options that appear dimmed.

NOTE With the **IP Address** column displayed, you can edit the IP address for a managed device by double-clicking the entry for the device and entering a new value.

Sort entries on the **Devices** page by clicking a column heading. **Status** and **Device type** are not sortable columns.

In the **Tools** column, you can sort entries by clicking an icon in the column heading. Tool icons that indicate and provide access to mailbox and gatekeeper registration, MCU and recorder affinity, and license key status are available for sorting entries.

Device Status

An icon appears for each device in the **Status** column of the **Devices** page depicting device status such as discovered or rebooting.

If you did not allow Avaya Video Conferencing Manager to attempt to manage devices during the initial discovery, all discovered devices appear with the **Discovered** status icon . To enable Avaya Video Conferencing Manager to manage these devices, click the device entry, , and **Manage selected device**. Read more at Discovering Devices.

Device Tools

One or more of the following icons may appear in the **Tools** column of the **Devices** page.

	Appears only if you enabled integration with a third party scheduling application and only for managed devices that can be scheduled in a call using this feature. Read more at Integrating a Third Party Scheduler.
	Indicates whether affinity to an MCU is set on the device. Read more at MCU Affinity.
	Indicates whether affinity to a recorder for recording video conferences is set on a device. Read more at Recorder Affinity.
	Indicates whether the device has been registered with a gatekeeper. Read more at Registering a Device to a Gatekeeper
	Indicates whether the device has a valid (green), expiring (yellow), or expired (red) license key. Available for LifeSize devices only. Read more at Managing Device License Keys.
	View the device's calendar. Read more at Scheduling a Conference in Avaya Video Conferencing Manager.
	Opens a text box for sending a message to the device. The message appears in the display of the device. Read more at Sending a Message to a Device.

Browsing Devices

Click to open the **Browse** window at any time to choose a category of devices to view. The number of devices (*x*) in that category and the total number of devices (y) appear on the **Devices** page heading as **Devices (**x*/y***)**. The total can include devices that are managed; discovered; discovered, but login failed; and external devices. To search for a single device, enter any alphanumeric string in the **Search** field at the top of the page. This field is case-sensitive.

Browse by	Description
Status	The ALL folder shows all devices that are discovered, managed or attempting to be managed, and external devices. You can view the following categories: • all managed devices • managed devices that are available, unavailable, offline, rebooting, and failed login • discovered devices (unmanaged and login failed) • devices in the managing state: Avaya Video Conferencing Manager is attempting to manage the device • external devices
Device Type	The ALL folder lists all managed devices by device type. You can browse devices by type, and refine the view by selecting a make, model, and software version. Device types include the following: • video communications systems • phones • MCUs • gatekeepers • gateways • video conference recorders
Activity	All managed devices with activities described by the following selections: • all devices with scheduled calls or: - with a call in progress (refreshed every 30 seconds on screen) - with no call activity - used at least once in a call since they were first managed by Avaya Video Conferencing Manager - scheduled calls within the next 24 hours, week, or month • all devices with upgrades: - in progress - scheduled to occur within the next 24 hours, week, or month • all devices with offline events or that have the following offline activity: - currently offline - scheduled to be taken offline within the next 24 hours, week, or month • all devices with scheduled template applications or all devices with templates scheduled within the next 24 hours, week, or month

Browse by	Description
Registration	The ALL folder shows all managed devices with a registration status or LifeSize license status in the following subcategories: • devices registered or unregistered to gatekeepers • devices registered or unregistered to a mailbox for installations integrated with a third party scheduling application • devices registered or unregistered to a SIP registrar • devices registered or unregistered to Skype (applies to LifeSize Passport only) • LifeSize video communications systems with licenses expiring within the next week, month, or year, and expired licenses • all devices that are assigned affinity to an MCU • all devices that are assigned affinity to a video conference recorder
Subnet	All managed devices by subnet

NOTE The Device Type, Activity, Registration, and Subnet Browse by categories show only managed devices.

Refreshing Device Information

Refresh the following information that appears on the **Devices** page:

- For all devices on the **Devices** page, click .
- For a single device, click the device entry, ; **Configuration**, and **Refresh device**.
- For recently added devices, in **Actions**, click **Scan Network** and then **Submit**. This procedure initiates discovery of devices added to the network since the last time devices were discovered.

Device Management Overview

Available options depend on the device's type and status. Click a device entry and to view the tasks available for that device.

NOTE A task that appears unavailable for selection indicates that the user does not have permission to perform that task. Read more at Managing Device Permissions Groups for Custom Roles.

Menu Option	Submenu Option	Device Type	Description
Manage selected device	None	All discovered, but unmanaged devices	This option appears if you clear the **Start managing once discovered** checkbox during device discovery. Read more at Discovering Devices.

Menu Option	Submenu Option	Device Type	Description
Discover registered devices	None	Gatekeepers	Refer to Discovering Devices Registered to a Gatekeeper.
Configuration	**View details**	All managed and external devices	Refer to Device Details for viewing device details of managed devices. Refer to Managing External Devices for viewing details of an external device.
	Launch browser interface	All managed devices	Launches the device's browser interface to access the configuration options on that device.
	Change password	All managed devices except gatekeepers, gateways, LifeSize Networker, LifeSize Multipoint, Radvision MCUs, Sony PCS-XG80, LifeSize Video Center, and LifeSize Bridge	Refer to Managing Device Passwords.
	View alarms	Managed video and voice communications devices except Sony PCS-XG80	Opens the **Alarms** page and shows the alarms for the device. Refer to Managing Device Alarms.
	Create template	Managed Avaya, LG, and LifeSize video systems only	Creates a configuration template from an existing managed video system. Refer to Using Templates to Configure Devices.
	Refresh device	All managed devices	Refreshes the selected device's information. Read more at Refreshing Device Information.
	On demand conferences	LifeSize Bridge	Shows all available on demand conferences. Read more at On Demand Conferences in LifeSize Bridge.
	Default conference settings	LifeSize Bridge	Allows you to configure default conference settings for the selected LifeSize Bridge.

Menu Option	Submenu Option	Device Type	Description
Events	**Join conference**	Video and voice communications systems only	Joins the device to a call in progress.
	Schedule call	Managed video or voice devices, MCUs, and video conference recorders	Schedules a call. Select multiple devices with the Ctrl or Shift keys and choose **Schedule call**. Read more at Scheduling a Conference in Avaya Video Conferencing Manager.
	Schedule upgrade	All managed video and voice devices except Sony PCS-XG80	Schedules a software upgrade for the device (requires an available upgrade package). Refer to Upgrading Devices. If you select multiple devices of the same make and model using the Ctrl or Shift keys, choosing this task opens the **Schedule upgrade** page and adds the devices to the upgrade.
	Take device offline	All managed devices except gatekeepers, gateways, LifeSize Networker, and video conference recorders	Prevents a device from being scheduled for a call, an upgrade, and, if applicable, a template event during the specified offline time period. Avaya Video Conferencing Manager continues to manage the device but does not allow access to device settings. Read more at Scheduling Offline Time for a Device.
	Bring device online	All managed devices except gatekeepers, gateways, LifeSize Networker, video recorders, and LifeSize Bridge	Available for a device that is taken offline.
	View calendar	Managed video or voice devices, MCUs, and video recorders	Shows the calendar of scheduled events for the device.
	Show call statistics	Managed video and voice devices; does not include MCUs	Shows the call statistics for a device that is currently in a call.
Update password	None	All managed devices except gatekeepers and LifeSize Networker	Refer to Managing Device Passwords.
Reboot device	None	All devices except gatekeepers, video recorders, and Sony PCS-XG80	Reboots the device. The device must not be in use. You can safely reboot the device when the **Responding** icon appears as the device status.

Menu Option	Submenu Option	Device Type	Description
Delete device	None	All devices	Deleting a device results in the following: • Avaya Video Conferencing Manager removes the device from the **Devices** page and from all scheduled calls and events in which the device is a participant. • If the device is a participant in a call scheduled through an integrated third party scheduler, Avaya Video Conferencing Manager notifies the meeting organizer of the change. • If the device is the host in a scheduled call, Avaya Video Conferencing Manager deletes the call. • Avaya Video Conferencing Manager also deletes any device backups created from the **Templates** page.

Device Details

View details for a managed device by double-clicking the device name on the **Devices** page or by clicking , **Configuration**, and **View details**. (To locate a managed device, click and in **Browse by**, select **Status**.)

NOTE When you schedule a call for the device from the **Schedule Call** page, each device added to the **Schedule Call** page appears as a link. Click the link to open the **Device details** page.

From the **Device details** page, you can do the following:

- View system information and edit the system name and locale settings.
- Set the default service prefix for a LifeSize or Radvision MCU. Refer to Setting a Default Service Prefix for an MCU.
- Specify northbound settings for forwarding traps for a device. Refer to Forwarding SNMP Traps with Northbound Settings.
- View Device Status and Device Tools.
- For LifeSize, Avaya, or LG video systems, you can also access many of the configuration preferences that are available in the device's web administration interface.
- For LifeSize Video Center, set the recording key.

- Set the hierarchy that appears on the directory screen for LifeSize, Avaya, or LG video systems when a user chooses to browse the corporate directory hierarchically. Refer to Managing Device Groups.

NOTE You can enter only the following characters in text boxes on the **Device details** page: A-Z a-z 0-9 ~ ! @ # $ % ^ & * ( ) _ - + = { } | \ < , > . ? / ; : \

Managing External Devices

Add an external device to the **Devices** page to identify devices that are frequently used in calls but may be unreachable by Avaya Video Conferencing Manager, such as a device that you do not wish to manage in Avaya Video Conferencing Manager or a device not on your organization's network. The new device then becomes available when you schedule a call in the **Events** page. The device also appears on the **Devices** page as an external device.

Adding an External Device

1. On the **Devices** page in **Actions**, select **Add a new external device**.
2. Click **Submit**.
3. Enter the details for the new device. The system name and IP address are required.
4. Click **Save**.

Listing External Devices

1. On the **Devices** page, click .
2. In **Browse by**, click **Status**.
3. Click **External**.

Editing Details for External Devices

Access the **View details** page for an external device and enter additional information such as the device make, model, and location, or other information that may be useful when including the device in a call.

1. On the **Devices** page, click .
2. In **Browse by**, click **Status**.
3. Click an external device.
4. Click , **Configuration,** and **View details**.

You can also join an external device to an existing conference call or delete the device from the **Devices** page. Refer to Device Management Overview.

NOTE With Microsoft Exchange Server integrated, Avaya Video Conferencing Manager can automatically add external devices to the **Devices** page. Read more at Specifying a Preferred Method of Participation.

Managing Device Passwords

When Avaya Video Conferencing Manager attempts to manage a device, it uses the default password that you specify on the **Passwords** page. Refer to Specifying Default Passwords for Device Management. If the device does not use that default password, the device appears on the **Devices** page with in the **Status** column indicating that the login failed. You must update the password stored in the Avaya Video Conferencing Manager database for that device before you can manage the device.

NOTE The also appears after a device is managed if the device's password is changed using a mechanism other than Avaya Video Conferencing Manager (for example, at the command line interface for the device).

Updating a Device Password in Avaya Video Conferencing Manager

Updating a password for a device in Avaya Video Conferencing Manager changes the password stored for that device in the Avaya Video Conferencing Manager database. It does not change the password stored on the device.

1. On the **Devices** page, click the name of the managed device.
2. Click and **Update Password**.
3. Enter a username and password.
4. Click **Update**.

Changing a Device Password on the Device

You can use Avaya Video Conferencing Manager to change the password stored on a device only if the device is managed in Avaya Video Conferencing Manager. Changing a password on a managed device changes the password stored on the device and automatically updates the password that Avaya Video Conferencing Manager stores in its database and uses to contact the device.

1. On the **Devices** page, click the name of the managed device.
2. Click , **Configuration**, and **Change Password.**
3. Enter and confirm the new password.
4. Click **Update**.

Sending a Message to a Device

Send a message to a managed video device to appear in the display connected to the device. The message appears in a dialog box with an **OK** button for users to acknowledge and close the message.

NOTE This feature is available only for managed Avaya, LG, LifeSize, Polycom, and Tandberg video communications systems. If not acknowledged, the message closes after 10 seconds on Avaya, LG, and LifeSize video communications systems only.

To send a message, follow these steps:

1. On the **Devices** page, use the **Browse** window to list all managed devices.
2. Locate the entry for the device and click in the **Tools** column.

NOTE If this icon does not appear, click and ensure that **Send message** is selected in the **Tools** section.

3. Enter a message. Only ASCII characters are allowed. The maximum number of characters allowed depends on the device's make:
   - Avaya: 200
   - LG: 200
   - LifeSize: 200
   - Polycom: 100
   - Tandberg: 40

NOTE To send the same message to multiple devices, use the Shift or Ctrl keys to select the devices and then click . The maximum number of characters allowed when multiple devices are selected is limited to the make with the fewest number of characters allowed.

4. Click **Send message**.

MCU Affinity

Use cascading MCUs to connect calls between two groups of participants. Each groups' communication is channeled through one MCU, and the MCUs pass the bundled communication between each other, greatly reducing the bandwidth needed for the groups to communicate with each other. To use this feature when scheduling a call, the devices in the call must be assigned affinity to an MCU.

Assigning MCU affinity to devices has additional benefits. If you schedule a call in Avaya Video Conferencing Manager and none of the devices has the capacity to host the call, Avaya Video Conferencing Manager prompts you to add an MCU and asks if you would like Avaya Video Conferencing Manager to make the selection for you. Avaya Video Conferencing Manager makes the selection based first on the MCU affinity of the participating devices, if assigned.

You cannot schedule cascading MCUs through a third-party scheduler. If you schedule more than one MCU, Avaya Video Conferencing Manager selects one based on the MCU affinity of the participating devices. If you do not schedule an MCU and one is needed to place the call, Avaya Video Conferencing Manager adds an MCU based on the MCU affinity of the participating devices.

Follow these steps to assign MCU affinity to a device:

1. On the **Devices** page, use the **Browse** window to show a list of managed devices.
2. Locate the entry for the device and click in the **Tools** column.

NOTE If this icon does not appear, click and ensure that **Set the MCU affinity** is selected in the **Tools** section. MCU affinity is not available for external devices.

---

3. In the **Set the MCU affinity** dialog box, select an MCU. If a managed MCU does not exist in Avaya Video Conferencing Manager, **Select the MCU** is not available.
4. Click . The MCU affinity icon in the device entry changes to indicate that MCU affinity is set for the device.

NOTE Click to clear affinity.

Read more at Using Cascading MCUs.

Recorder Affinity

If your installation includes managed video conference recorders, assign each video system affinity to a recorder to enable Avaya Video Conferencing Manager to automatically select a recording host when a meeting organizer schedules a call through a third party scheduler or from the **Events** page. Scheduling calls may fail if an appropriate recorder is not available. Avaya recommends that if your installation includes managed video recorders, that you set affinity to these recorders on all applicable managed video systems.

If your installation includes LifeSize Video Center and Avaya systems supported with LifeSize Video Center, set recorder affinity on the Avaya systems to LifeSize Video Center; and define a default recording key. Assigning a default recording key to use when a Avaya video system is the recording host in a call ensures that if recorder affinity is not assigned, Avaya Video Conferencing Manager can automatically select a LifeSize Video Center to use and associate a recording key.

When a meeting organizer or a Avaya Video Conferencing Manager user schedules a call to be recorded, Avaya Video Conferencing Manager chooses a managed video conference recorder based on assigned recorder affinity:

- If LifeSize Video Center is managed by Avaya Video Conferencing Manager and a participant in the call is a Avaya system supported with LifeSize Video Center, Avaya Video Conferencing Manager chooses that system as the recording host. If that system is assigned affinity to a managed LifeSize Video Center, LifeSize Video Center is used to record the call with the recording key specified at the time the affinity was assigned. If recorder affinity is not assigned to the Avaya recording host, Avaya Video Conferencing Manager selects an available LifeSize Video Center and uses the default recording key, if set.
- If none of the participants in the call are Avaya systems that are supported with LifeSize Video Center, or if LifeSize Video Center is not managed in Avaya Video Conferencing Manager, a recorder is selected based on affinity assigned to other managed recorder models.

Setting a Default Recording Key to use with a LifeSize Video Center

Complete the following steps to associate a default recording key to use when a Avaya video system is the recording host in a call and affinity to a LifeSize Video Center has not been set on the system:

1. On the **Devices** page, use the **Browse** window to show a list of managed LifeSize Video Center devices.
2. Double-click the LifeSize Video Center entry; or click the device entry, , **Configuration,** and **View details**.
3. On the **System information** tab, enter a recording key in **Recording key**. The recording key must be one that already exists on the LifeSize Video Center.
4. Click **Save**.

Assigning Recorder Affinity

1. On the **Devices** page, use the **Browse** window to show a list of managed video communications systems.
2. In the **Tools** column, click for the video system.
3. In the **Set the recorder affinity** dialog box, choose a video recorder.

NOTE Only managed video recorders that are supported with the system appear on this list.

4. If you select a LifeSize Video Center, **Set recording key** appears. Enter a key that is available on the selected LifeSize Video Center.

NOTE A default key appears in this text box if you set a default key in Setting a Default Recording Key to use with a LifeSize Video Center. The recording key must be one that already exists on the LifeSize Video Center.

5. Click **Set the recorder affinity**.

NOTE Clear a device's recorder affinity by clicking and then **Clear the recorder affinity**.

Setting a Default Service Prefix for an MCU

Set a default service prefix for a managed LifeSize or Radvision MCU from the **Device details** page. A service prefix identifies a service created on the MCU. For information about creating services on the MCU, refer to the product documentation that accompanies the MCU.

1. On the **Devices** page, use the **Browse** window to list MCUs.
2. Double-click the MCU entry; or click the MCU entry, , **Configuration**, and **View details**.

NOTE You can also change the service prefix on the **Device details** page when you schedule a call. From the **Schedule Call** page, click the link to open the **Device details** page. Changing the service prefix on the **Device details** page when scheduling a call changes the prefix only for that call.

3. On the **System information** tab in the **Device details** page, locate the **Generic properties** page.

4. In **Service prefix**, click the service prefix you wish to use. The maximum bandwidth and maximum participants for that prefix appear below the list.

NOTE If the service prefix you select is subsequently deleted on the MCU, Avaya Video Conferencing Manager chooses the next available prefix with the highest bandwidth allowed. If no services are registered on the MCU, a scheduled call with this MCU fails.

5. Click **Save**.

Forwarding SNMP Traps with Northbound Settings

Avaya Video Conferencing Manager supports management of video communications devices through SNMP, a standard mechanism for tracking configuration and status of a system. SNMP allows for connection to third-party management frameworks.

Using SNMP version 3, you can send SNMP traps from Avaya Video Conferencing Manager to a management system such as a northbound SNMP receiver. This functionality is useful to networking companies using trap complexes. You can configure one or more SNMP trap hosts and send copies of traps for further use with data mining tools to show trends on the network.

Trap forwarding in Avaya Video Conferencing Manager is available only for managed video and voice devices. This feature is not available for managed gatekeepers, gateways, video conference recorders, and MCUs.

You can specify external SNMP trap destinations to which Avaya Video Conferencing Manager forwards traps from a single managed device using the **Northbound** tab on the **Device details** page of the device. You can also use the **Northbound Settings** page in Avaya Video Conferencing Manager Administrator to specify global trap destinations to forward all traps from all managed video and voice devices or to enable or disable trap forwarding.

If you configure global trap destinations, each global trap destination is indicated by on the **Northbound** tab on the **Device details** page of each managed video and voice device. You cannot edit a global trap destination from the **Device details** page.

By default, trap forwarding is enabled. To disable trap forwarding, clear the **Enable Avaya Video Conferencing Manager Northbound Settings** checkbox on the Northbound Settings page in Avaya Video Conferencing Manager Administrator and refresh your browser. If you disable trap forwarding, the **Northbound** tab on the **Device details** page does not appear.

NOTE If you configure global trap destinations in Avaya Video Conferencing Manager Administrator and trap destinations on the **Device details** page for a single device, Avaya Video Conferencing Manager forwards traps for that device to all trap destinations specified in both Avaya Video Conferencing Manager Administrator and on the **Device details** page.

Follow these steps to specify a trap destination to forward traps from a single device:

1. On the **Devices** page, use the **Browse** window to list managed devices.
2. Double-click the device entry; or click the device entry, , **Configuration**, and **View details**.
3. Click the **Northbound** tab.

NOTE If trap forwarding is disabled in Avaya Video Conferencing Manager Administrator, the **Northbound** tab on the **Device details** page is not available.

4. Click **Add**.
5. Enter the following information about the SNMP trap destination:
   - IP address
   - port number on which the remote SNMP manager is listening for traps
   - username (not to exceed 40 characters)
   - password (not to exceed 40 characters)
6. Click **Save**. The entry appears in the table above **Add**.

NOTE To edit or delete an SNMP trap destination, click or in the **Actions** column.

Managing a Device Through Email

If you integrated Microsoft Exchange Server with Avaya Video Conferencing Manager, Avaya Video Conferencing Manager administrators can send management commands to managed video devices by email. The **To** field of the email message must contain the email address of one or more managed devices. Administrators can send an email as plain text, HTML, or rich text. The **Subject** field must contain one of the following commands. The commands are not case-sensitive.

Command	Applies to these Makes	Action Executed on the Device
REBOOT	Avaya LG LifeSize Polycom Tandberg	Reboots the devices.
CALL	Avaya LG LifeSize Polycom Tandberg Sony	Places a conference call that includes the list of devices to which the email is sent. The appears in the **Type** column on the **Events** page to identify an adhoc call placed through email using this command. NOTE: This command cannot be used to add devices to a conference call in progress.
HELP	Avaya LG LifeSize Polycom Tandberg Sony	Sends a reply email that lists and describes the commands that can be sent to the device in an email message. A single reply is sent even if the HELP command is sent to multiple devices.
HANGUP	Avaya LG LifeSize Polycom Tandberg Sony	(Does not apply to MCUs.) Disconnects the list of devices to which the email is sent if these devices are in a call. If one of the devices is hosting a call, then all participants connected to that host in the call are also dropped.
BACKUP BACK-UP BACK UP	Avaya LG LifeSize	Backs up the current device settings as a template.
CALLSTATS CALL STATS CALL STATISTICS	Avaya LG LifeSize Polycom Tandberg Sony	Retrieves call statistics.

Command	Applies to these Makes	Action Executed on the Device
DESCRIBE DESC	All managed devices	Retrieves the details of the devices. This information appears on the **Device details** page of a managed device.
MESSAGE	Avaya LG LifeSize Polycom Tandberg	Shows a message in the display of the video system. Use only ASCII characters. Enter the message in the body of the email. Delete signature information or other text that automatically appears in the body of the message. Avaya Video Conferencing Manager truncates messages that exceed the following number of characters: Avaya, LG, and LifeSize: 200 Polycom: 100 Tandberg: 40
SNAPSHOT	Avaya LG LifeSize	Retrieves the current video snapshot on the device as a .jpg attachment to a reply email.
AUTOSH	Avaya LG LifeSize	Executes a command line interface (CLI) command. Enter AUTOSH in the **Subject** field and the CLI command in the body of the message (for example, `get system name`).

Avaya Video Conferencing Manager sends an individual response email (success or failure) to indicate the result of the action taken on each of the devices. If Avaya Video Conferencing Manager does not recognize any of the emails, then no action or response email is sent. Email commands are not supported with external devices.

The **Conference audit report** available from the **Reports** page includes **EMAIL** as a call source type for calls initiated through email commands. The **User audit report** reflects the conferences initiated by users using email commands. Read more at Generating Reports.

You can disable this feature by clearing **Enable device management through email** on the Mail Integration Settings page in Avaya Video Conferencing Manager Administrator.

Managing Device Groups

Group devices into folders in Avaya Video Conferencing Manager to do the following:

- Create and set a default hierarchical group of managed devices to appear in the directory for all managed Avaya, LG, and LifeSize video systems when the user chooses to browse the corporate directory hierarchically. You can also create more than one group and select the group that appears in the directory for an individual system. Devices that are available for placing into a hierarchical group include managed video and voice devices, LifeSize Desktop installations, external devices, and on demand conferences.

  NOTE Assign LifeSize Desktop installations to a group from the **LifeSize Desktop** page. You must create the group first from the **Devices** page by following the instructions in this section and then add the installations from the **LifeSize Desktop** page.

- Specify the tasks that a custom role can perform on managed and external devices in a folder. For example, in Avaya Video Conferencing Manager Administrator, you can create a custom role for users in a specific geographical region. From the **Devices** page, group all devices in that region into a folder, assign the custom role that you created for that region to the folder, and choose which tasks that custom role is authorized to perform on the devices in that folder. Read more about custom roles at Role Management Settings.

Creating a Directory Group

Create a device group that users of managed devices can use to browse the corporate directory hierarchically:

1. On the **Devices** page, click .
2. In the **Device groups** window, click **Manage groups**.
3. Click **Create group**.

   NOTE The name of the group is restricted to the following characters: A-Z a-z 0-9 ~ ! @ # $ % ^ & * ( ) _ - + = { } | \ < , > . ? / ; : \

   The name of the group appears in the pane below **Group name**. This name represents the top of the hierarchy. It does not appear on the directory screen when you set it as the default. You cannot assign devices to it. You create subfolders under this folder and add devices to the subfolders to form the hierarchy that appears in the directory screen.
4. In the pane below **Group name**, click the group name.
5. Click and **Create folder**.
6. Enter the name of the folder.

7. Select the devices that you wish to include in the folder. Use the **Search** box to search for a device in the list that appears.

   NOTE A device can reside in only one folder per group. A device appears unavailable if it is already assigned to another folder. Mouse over the unavailable device to view text that identifies the folder to which the device is assigned. Click the checkbox to override the assignment and assign the device to the currently selected folder.

8. Create additional folders to complete the hierarchy. Click the group name or a folder and repeat steps 5 - 7.
9. To set a group as the default group to appear on the directory screen when a user chooses to browse the corporate directory hierarchically, select the group in **Group name**, and then click **Set as default**. The button label changes to **Reset as default** to indicate that this is the currently selected default group. If you wish to change the default group or have no group appear in the corporate directory by default, click **Reset as default** to remove this group as the default selection.

Modifying a Directory Group

Modify a directory group or its folders as follows:

- To rename a directory group, select the group in **Group name** and then click **Rename**.
- To delete a directory group, select the group in **Group name**, and then click **Delete**.
- To delete or rename a folder, click the folder, , and **Rename folder** or **Delete folder**.

NOTE Dragging and dropping folders is not supported.

If you modify a group, the changes appear on the directory screen of the device using that group based on the refresh interval set in **Administrator Preferences : Directory : LDAP : LDAP Refresh** on the device. The default refresh interval set by Avaya Video Conferencing Manager when it discovers and manages a device is 12 hours.

In the **Device groups** window, you can view the structure of a group and the device assignments in each of its folders by selecting the group name in **Browse by**. The group appears in the pane below the list.

Overriding the Default Directory Group

Follow these steps to override the default directory group on an individual video system, if one is set, or to specify a directory group on an individual system:

1. On the **Devices** page, browse for the device to which you wish to assign a directory group.
2. Click the device entry.
3. Click , **Configuration**, and **View details**.
4. In the **Device details** page, ensure that the **System information** tab is selected.
5. In **Corporate directory**, click the name of the directory group that you wish to appear as the hierarchical group on the directory screen for this device when the user chooses to browse the directory hierarchically.
6. Click **Save**.

Managing Device Permissions Groups for Custom Roles

Follow these steps to place devices in folders, assign a custom role to the folder, and choose which tasks the role is authorized to perform on those devices:

1. On the **Devices** page, click .
2. In the **Device groups** window, click **Manage IT group**.
3. In the **Manage IT group** window, click the **IT Group** folder.
4. Click and **Create folder**.
5. Enter the name of the folder.
6. Select the devices that you wish to include in the folder. Use **Search** to search for a device in the current list.

NOTE A device can reside in only one folder. A device appears unavailable if it is already assigned to another folder. Mouse over the unavailable device to view text that identifies the folder to which the device is assigned. Click the checkbox to override the assignment and assign the device to the currently selected folder.

7. Assign a role to a folder and choose the tasks that a user assigned to the role is authorized to perform on the devices in the folder:
   a. Click a folder, , and **Manage permissions**.
   b. In the **Manage permissions** window, click the custom role that you wish to assign to the folder.

   NOTE The Administrator, Engineer, and Operator roles appear in this list for reference only to show the tasks that these roles are authorized to perform on devices.

   c. Select the authorized tasks for the selected role.
8. You can modify folders as follows:
   a. To delete a folder, click the folder, , and **Delete folder**.
   b. To rename a folder, click the folder, , and **Rename folder**.

   NOTE Dragging and dropping folders is not supported.

Populating the Phonebook on Tandberg Systems

When Avaya Video Conferencing Manager manages and refreshes Tandberg video communications systems, it uses FTP to push a list of managed video communications devices to these systems. The list appears in the Phonebook of the managed Tandberg systems.

Managing Device Alarms

Use the **Alarms Configuration** page in Avaya Video Conferencing Manager Administrator to choose which alarms Avaya Video Conferencing Manager reports. Read more at Alarms Configuration and Alarms by Category. View and manage alarms on the **Alarms** page.

Viewing Alarms

Access the **Alarms** page in one of the following ways:

- On the **Dashboard**, click a category in the **Alarms** section to view a list of alarms in that category.
- On the navigation bar, click .
- On the **Devices** page, click a managed video or voice device. Click , **Configuration**, and **View alarms**.

NOTE If **View alarms** does not appear, this feature may not be supported for that device model. Refer to View alarms for a list of supported models.

When you access the **Alarms** page, the most recent 100 entries appear. To view the next or additional 100 entries, use the page numbers or **Go to page** box at the bottom of the page. Use the **Search** box at the top of the page to search for information only on the current page of entries.

Click any column heading to sort all alarms by ascending or descending order based on the information in that column.

You can choose how alarms appear on the **Alarms** page in the following ways:

Columns	Click to specify the columns of information that appear for all alarm entries.
Browse	Click to show a list of alarms based on a single criterion and associated value, for example, all alarms for which the severity is HIGH. In **Browse by**, click a criterion and then click a value in the menu that appears below the list. The list of alarms that appears refreshes automatically when you click a value. You can select multiple values by using the Shift or Ctrl keys. Click **Show all** to clear the list and show all alarms.
Refresh	Click to refresh alarm entries on the current page.
Search	Click to search for alarms based on one or more selected criteria and associated values. Click **Show all** to clear a search and show all alarms.

Choosing a Management Option

Manage a single alarm (or multiple alarms with Shift or Ctrl) these ways:

- View alarm details. Double-click and alarm entry; or click an alarm entry, , and **View details**.
- Acknowledge an alarm. Click an alarm entry, , and **Acknowledge alarm**. The alarm becomes inactive.

NOTE View acknowledged alarms in the **Browse** window by clicking **Acknowledged by** in **Browse by**.

You can also click an alarm entry, , and **Acknowledge alarm with resolution**. Enter information (up to 500 characters) about how the issue was resolved.

NOTE Users must be authenticated to acknowledge alarms, even if they are not logged in to Avaya Video Conferencing Manager when doing so (for example, when acknowledging an alarm from the email notification).

- Unacknowledge an acknowledged alarm. Use the **Browse** window to list acknowledged alarms. Click an acknowledged alarm entry, , and **Unacknowledge alarm**.
- Assign an owner to an alarm by clicking an alarm entry, , and **Assign alarm**. Choose the person to which to assign the alarm from the corresponding list that appears and then click **Assign alarm**. To assign yourself as the person responsible for resolving the alarm, click the selected alarm entry, , and **Own alarm**. Your name appears in the **Owner** field for that alarm. That alarm then appears in **My active alarms** on the Dashboard.

NOTE You can also search or view alarms by owner with the **Search** and **Browse** windows.

- Send alarm information to another user by clicking the alarm entry, , and **Forward alarm**. Enter the email address of the recipient and click **Forward alarm**.

Exporting Alarms

Use **Export** to export all alarms as either a CSV or PDF file. To export selected alarms, use Shift+click or Ctrl+click to select the alarms, click one of the selected alarms, , and **Export selected - CSV file format** or **Export selected - PDF**.

Using Templates to Configure Devices

Templates in Avaya Video Conferencing Manager are stored configurations for video systems that you can apply to a single device or multiple devices simultaneously. Use templates to achieve any of the following goals:

- Configure new video communications systems.
- Improve troubleshooting and support capabilities. Compare a device's configuration with a template to determine discrepancies; apply a template to resolve a problem associated with a changed configuration; or ensure that systems are set to the company defaults.
- Back up and restore the configuration of a device.
- Adhere to security policies by periodically applying templates. For example, you can create a template that prevents unauthorized video access to conference rooms by disabling automatic call answering; applying encryption in calls; disabling control of cameras by far end users; and disabling automatically starting a presentation when a presentation device is connected to a system.

Create a new template and specify the settings manually, or create a template based on an existing device. For a new template, you can specify template parameters based on the device's make, software version, and model, or specify a template that contains only common parameters for all models or all models of a selected make.

The following restrictions apply to templates:

- Templates are supported for the following makes:
  - Avaya
  - LG
  - LifeSize
- Create templates for managed LifeSize Desktop installations on the **LifeSize Desktop** page or the **Templates** page.
- Refer to the release notes for Avaya Video Conferencing Manager for a list of device software versions for which template support is available.
- Not all configuration preferences that are available in the device user interface are available in templates.
- You can enter only the following characters in text boxes when creating or editing templates:

  A-Z a-z 0-9 ~ ! @ # $ % ^ & * ( ) _ - + = { } | \ < , > . ? / ; : \
- Applying a template reboots the device to which it is applied after the application process is complete.

Creating and Editing Templates

1. Click on the navigation bar to access the **Templates** page.
2. In **Actions**, choose either **Create template** to create a new template or **Create template from device** to create a template based on the configuration of an existing device.
3. Click **Submit**.
4. Depending on the type of template you want to create, do one of the following:
   - New template: enter the details for the template (name, make, version, and model for the device).
   - Template from an existing device: select the device from which to create the template and enter a name for the new template.

   NOTE You can also create a template from an existing device from the **Devices** page by clicking the device, , **Configuration**, and **Create template**.
5. Click **OK**.
6. Configure the desired preferences.
7. Click **Save**. An entry for the template appears on the **Templates** page.

   NOTE Edit a template by double-clicking its entry on the **Templates** page or clicking its entry on the **Templates** page, , and **Edit template**.

Applying a Template

Apply a template immediately to one or more devices, or schedule a template application for a future date and time. Read more at Scheduling Template Applications and Comparisons. To apply a template immediately, complete the following steps:

1. On the **Templates** page, click the template entry, , and **Apply template**.
2. In the **Apply template** window, click the devices. Use the Shift or Ctrl keys to select multiple devices.
3. Click **OK**.
4. When the **Templates** dialog box appears, click **OK**.
5. Check for template application errors. In **Actions**, select **View logs** and click **Submit**.

   The **View logs** dialog box indicates the status of the operation. **Failed parameters** identifies parameters that were not updated correctly during the template application.

Comparing a Template

Compare a template immediately to an existing device's configuration, or schedule a template comparison for a future date and time. Read more at Scheduling Template Applications and Comparisons. To compare a template to an existing device's configuration immediately, complete the following steps:

1. On the **Templates** page, click the template entry, , and **Compare template**.
2. In the **Compare template with device settings** dialog box, select the device entry.
3. Click **OK**.

   The **Compare template with device settings** dialog box lists any differences between the template settings and the current settings on the device.

Deleting a Template

To delete a template that is not scheduled to be applied to a device, on the **Templates** page, click the template entry, , and **Delete template**.

Maintaining Devices

Upgrading Devices

To upload new software packages for your devices, follow these steps:

1. Download an upgrade package from the device manufacturer for the devices you wish to upgrade. Ensure that the package resides at a location on your network that is accessible to Avaya Video Conferencing Manager.
2. Click on the navigation bar to access the **Packages** page.
3. In **Actions**, choose **Upload packages** and click **Submit**.
4. Specify the make, model, and version of the package.
5. Enter the location of the software package or click **Browse** to navigate to it.
6. Click **Upload**.

   An entry for the package appears on the **Packages** page. Apply the software upgrade package immediately or schedule it for a later time. Refer to Scheduling a Device Software Upgrade.

NOTE To remove a package from the list, click the package entry, , and **Delete Package**.

Managing Device License Keys

Attempting to upgrade a device that requires a license fails if a current upgrade license key is not installed on the system. Contact Avaya Technical Services if you do not have a license key and need assistance.

All LifeSize video communications systems managed in Avaya Video Conferencing Manager show a key icon in the far right column of the **Devices** page. A green key indicates a valid license key. A yellow key indicates the license key will expire within a month, and a red key indicates an expired license key.

Update license keys manually by clicking the key icon. Or update multiple managed LifeSize video systems by using a batch file and the Avaya Video Conferencing Manager Administrator utility. Refer to Administering Avaya Video Conferencing Manager.

Backing up a Device

You can back up and restore configuration settings for individual LifeSize, Avaya, and LG video systems only.

NOTE A backup can only be restored on the device from which it was generated.

Backup and restore operations are an extension of the templates feature. Read more at Using Templates to Configure Devices. You can perform incremental backups over time and restore them at a later time from the **Templates** page.

Follow these steps to back up a device:

1. Click on the navigation bar to access the **Templates** page.
2. In **Actions**, choose **Backup device**.
3. Click **Submit**.
4. In the **Backup Device** dialog box, choose the device that you want to back up.
5. Enter a description for the backup.
6. Click **OK**.
7. Name the backup file and save it.

Restoring a Device from a Backup

1. Click .
2. In **Actions**, choose **Restore device**.
3. Click **Submit**.
4. In the **Restore device** dialog box, choose the device to restore.

5. Choose a backup.

NOTE A backup can only be restored on the device from which it was generated.

6. Click **OK**.

Registering a Device to a Gatekeeper

Register a managed device that supports the H.323 protocol to a managed gatekeeper as follows:

1. On the **Devices** page, use the **Browse** window to list all managed devices.
2. Locate the entry for the device and click in the **Tools** column.

NOTE If this icon does not appear, click and ensure that **Register with gatekeeper** is selected in the **Tools** section.

3. In the **Register with gatekeeper** dialog box, the **Gatekeeper** option is selected by default. In **Select the gatekeeper**, select a managed gatekeeper.
4. Click **Register**. The register with gatekeeper icon in the device entry changes to indicate that the device is registered to a gatekeeper.

NOTE Unregister a device by clicking and **Unregister**.

Managing User Accounts

Avaya Video Conferencing Manager supports multiple users and controls their access to functionality with roles. A role identifies the tasks that users assigned to the role are authorized to perform. Each user account is associated with one of the following predefined roles.

Administrator	Role with full access to all functionality, except editing and deleting all user accounts.
Engineer	Engineers can perform many of the same tasks as an administrator, except export or assign alarms; manage or modify device settings; create or apply templates; take devices offline; back up and restore a device; and access Avaya Video Conferencing Manager Administrator.
Operator	Operators can view alarms, device settings, and a list of users; and schedule and manage calls. Avaya Video Conferencing Manager assigns new users to the Operator role.

You cannot edit or delete the three predefined roles. Read more about access to specific functionality for each of these roles at User Role Access.

NOTE The superuser created during Avaya Video Conferencing Manager installation can edit and delete all user accounts, including administrators. Read more at User Authentication.

In Avaya Video Conferencing Manager Administrator, administrators can create additional custom roles and choose which page-level tasks a custom role can be authorized to perform. From the **Devices** page, an administrator can then assign device-level tasks to custom roles by grouping devices into folders, selecting a custom role to assign to the folder, and then choosing the tasks that the custom role is authorized to perform on devices in that folder. For more information about creating custom roles, refer to Role Management Settings. For more information about choosing device-level tasks for a custom role, refer to Managing Device Permissions Groups for Custom Roles.

NOTE Users of a third party scheduler can affect scheduling of calls. With Microsoft Exchange Server integrated, users can add external devices to Avaya Video Conferencing Manager without having a Avaya Video Conferencing Manager user account. Refer to Integrating a Third Party Scheduler.

Adding a User Account

Click on the navigation bar to manage user accounts. A list of defined registered users for Avaya Video Conferencing Manager appears.

New users are automatically assigned the Operator role. Refer to Modifying a User Account for details about changing roles.

Avaya Video Conferencing Manager categorizes defined users for Windows-based authentication. Depending on the type of user authentication you chose when installing the application, different options for user management appear.

Importing Users from Active Directory

If you chose Active Directory for user authentication when you installed Avaya Video Conferencing Manager, you can import Active Directory users by completing the following steps:

1. In **Actions**, choose **Import Active Directory users** and click **Submit**.

   The **Import Active Directory users** dialog box lists the first 100 users.

2. Import selected users in the list by clicking the names of the users you want to import. Use the **Search** box to search for a specific username and click **Submit**. You can also change any user account information (such as name, role, location, email, or contact number) by clicking **Next** after selecting the user and before completing the import.

3. Click **Import Selected** or click **Import all** to import all users that appear in the dialog box.

NOTE If you are using Active Directory for user authentication, you must change user passwords outside of Avaya Video Conferencing Manager.

Adding Users from ADAM

If you chose ADAM for user authentication when you installed Avaya Video Conferencing Manager, you can add new users as follows:

1. In **Actions**, choose **Add new user**, and then click **Submit**.
2. Enter information in all required fields. A red star appears next to a field that is required.

NOTE Passwords for ADAM or AD LDS users are case-sensitive.

3. Click **Save**.

Modifying a User Account

Only the superuser that you specified for logging in to Avaya Video Conferencing Manager when you installed the product can modify another user's account. Other administrators, engineers, and operators can modify their own accounts except their login name or user role. To modify an existing user account, follow these steps:

1. Click to access the **User Management** page.
2. Double-click the entry; or click the entry, , and **Modify User**.
3. In the **Modify user** dialog box, update the fields you wish to change. Only the superuser specified during installation can assign a different role to the user in this step. Refer to Managing User Accounts.
4. Click **Save**.

Deleting a User Account

Only the superuser that you specified for logging in to Avaya Video Conferencing Manager when you installed the product can delete a user account.

1. Click to access the **User Management** page.
2. Double-click the entry; or click and **Delete User**.
3. Click **Yes** to confirm the deletion.

Section 3: Scheduling Events

Click on the navigation bar to access the **Events** page, where you can schedule calls and other device events in the **Actions** list.

Event	Actions list command	Read more
Calls	Schedule Call	Scheduling Conferences
Device software upgrade	Schedule Upgrade	Scheduling a Device Software Upgrade
Template applications	Schedule Template	Scheduling Template Applications and Comparisons
Taking a device offline	Schedule device offline	Scheduling Offline Time for a Device

NOTE You can also schedule a call, an upgrade, or taking a device offline from the **Devices** page: click the device entry, , **Events**, and choose the option.

With an integrated third party scheduler, users can schedule video or voice calls in Avaya Video Conferencing Manager with the third party scheduling application. Read more at Scheduling Conferences in Microsoft Outlook and Scheduling Conferences in Google Calendar.

Choose an option in the **Display** list to view a list of events and do the following:

Restart a terminated or completed call.	Click the event entry, , **Dial this call again**, and **Call Now**.
View details of an event.	Double-click the event entry; or click the event entry, , and **View Details**.
Edit details of a scheduled event.	Click the event entry, , **Edit Details**, and **Apply changes**.
Delete a scheduled event.	Click the event entry, , and **Delete Schedule**.

Icons for calls, devices, templates, or upgrades appear in the **Status** column. The following event icons can appear in the **Type** column to indicate additional details about an event:

	A recurring event.
	A call scheduled from a third party scheduling application that is integrated with Avaya Video Conferencing Manager.
	An adhoc call initiated by a Avaya Video Conferencing Manager administrator using the email-based CALL command. Refer to Managing a Device Through Email.
	A scheduled call that includes a managed video conference recorder.
	A completed call that included a managed video conference recorder, but the recording failed.
	A completed call that included a managed video conference recorder and the recording succeeded.

Scheduling Conferences

Schedule and manage conferences in Avaya Video Conferencing Manager or from a third party scheduler:

- Scheduling a Conference in Avaya Video Conferencing Manager
- Scheduling Conferences in Microsoft Outlook
- Scheduling Conferences in Google Calendar
- Adding a Device to a Scheduled Conference
- Modifying Scheduled Conferences
- Using Cascading MCUs
- Viewing a Call in Progress
- On Demand Conferences in LifeSize Bridge
- Port Use

Calls that are successfully scheduled appear on the **Events** page when you show all scheduled events or scheduled calls. In the **Display** list, select **All scheduled events** or **All scheduled calls**.

Calls involving managed devices that were not scheduled through Avaya Video Conferencing Manager or an integrated third party scheduler appear on the **Events** page with the event name **Adhoc Conference**. Avaya Video Conferencing Manager captures statistics for adhoc conferences for reporting purposes.

Scheduling a Conference in Avaya Video Conferencing Manager

1. Click on the navigation bar to access the **Events** page.
2. In **Actions**, choose **Schedule Call** and then click **Submit**.
3. Enter the details for the call:
   a. Enter a name for the conference so you can identify it in a list of events on the **Events** page.
   b. Choose the reservation type:
      - Choose **Auto Launch** to automatically start the call at the scheduled time.
      - Choose **Reservation Only** to reserve devices for the call, but requires the call to be manually dialed. When reserved, you cannot schedule devices for maintenance or other purposes.
   c. Select the start and end date and time.
   d. Select **Auto disconnect** to end the call automatically when its scheduled time ends.
   e. Select **Alert before termination** to alert participants to the end of the call 5 minutes before the call is ended.

4. Add participants to the call:
   a. Click **Add Device** to show a list of managed devices.
   b. Add a displayed device by clicking it and clicking the **Add** button or by double-clicking the device. You can select multiple devices with the Ctrl or Shift keys. If you add more than two devices, Avaya Video Conferencing Manager automatically selects the first multipoint-capable device added as the host. If you add more devices to the call than the device currently hosting the call can handle, Avaya Video Conferencing Manager automatically reconfigures the call with a more capable host. You can also change hosts by dragging and dropping a participating device on the device currently selected as the host.
   c. To add an external device that is not available for selection in the **Add Device** dialog box, click **Add External Device**. Specify the protocol to use to connect to the device, enter the IP address or number to use to dial the device, and click .
   d. To record this call by including a managed video recorder, select **Record this call**. If you select a LifeSize Video Center, **Recording key** appears. The default key entered in Avaya Video Conferencing Manager appears, if recorder affinity was assigned. If you enter a different key, it must be a valid key in the selected LifeSize Video Center. Read more at Recorder Affinity.

NOTE If you are scheduling a call by clicking a video recorder from the **Devices** page, **Record this call** is automatically selected.

---

   e. Click **Add MCU** to add an MCU to the call. If none of the devices that you added to the schedule is capable of hosting the call and you do not add an MCU, a message prompts you to add an MCU to facilitate the call. MCU options include:
      - **Conference ID**. Enter a conference ID or leave blank. If you added LifeSize Bridge as MCU, click to select an on demand conference associated with the LifeSize Bridge. Read about how Avaya Video Conferencing Manager reserves ports at Port Use.
      - **PIN**. Manually enter a PIN (up to 10 characters) for the call or click to automatically generate a 5-digit PIN.

NOTE Unscheduled conferences that use a PIN do not show the PIN in the **Schedule call** dialog box when you view the call details from the **Events** page.

      - **Cascading MCUs**. Refer to Using Cascading MCUs.

NOTE Calls scheduled through Avaya Video Conferencing Manager that include LifeSize Bridge do not appear in the LifeSize Bridge Utility; calls scheduled through the LifeSize Bridge Utility do appear on the Avaya Video Conferencing Manager **Events** page.

---

f. Change the following call settings for a device added to the schedule by clicking the device entry in **Selected Devices** and then :

- Call Type (protocol)
- Bandwidth (**Auto** or choose a bandwidth from the list)
- Direction of the call (incoming or outgoing)
- Gateway (if applicable)
- Mute on connect
- Do not disturb (if applicable)
- *LifeSize Bridge only*: Reserved ports (**Auto** or choose a number from the list). **Auto** reserves the minimum number of ports required for scheduling the call. Read more at Port Use.

NOTE If your LifeSize Bridge supports expanding the conference to accommodate additional participants, set **Reserved ports** to **16** to activate this feature.

LifeSize Bridge only: Click to select the call layout. Lock the layout for the individual participant from the video device entry; or for all participants from the LifeSize Bridge entry.

g. The name and IP address of each managed participant that appears in **Selected Devices** is a link. Clicking the link opens the **Device details** page for that device to enable you to change configuration settings for that device. Read more at Device Details. Avaya Video Conferencing Manager automatically updates the call to reflect or adjust to any changes that you make to device settings that affect the call you are scheduling or editing (for example, changes to the protocols used in the call or the system names). Changes to MCU affinity from the **Device details** page do not affect the call.

5. Click **Recurrence** to set up a regularly occurring conference.

NOTE In an installation that uses ADAM for user authentication, you cannot schedule calls to recur beyond six months.

---

6. Click **Call Now** to begin the call immediately or **Schedule Call** to begin the call at the specified time. If the call is not configured properly, an error message prompts you to configure the call. Click **Configure** for Avaya Video Conferencing Manager to choose a valid configuration for the call.

NOTE You may encounter a configuration error that requires your intervention. For example, if one of the devices is set to a communication protocol that is incompatible with the protocol settings for other devices in the call, appears. Mouse over the icon to view descriptive text.

Adding a Device to a Scheduled Conference

1. Click to access the **Events** page.
2. In the **Display** list, select **All scheduled events** or **All scheduled calls**.
3. Click the event entry, , and **Edit Details**.

NOTE If the conference is recurrent, **Edit Details** appears as **Edit Details - this occurrence** or **Edit Details - this series**.

4. Click **Add device**.
5. Select a device from the list and click **Add** or double-click the device.
6. Close the **Add device** window.
7. Click **Apply changes**.

Modifying Scheduled Conferences

1. Click to access the **Events** page.
2. In the **Display** list, click **All scheduled events**.
3. Click the event entry, , and **Edit Details**.

   If the event is a recurring event, click **Edit details for this instance** or **Edit details for this series**.

   In the **Schedule Call** dialog box, you can change the type, bandwidth, and direction of a call, remove a participant from the call, alter the date or time, or select a new device to add to the call. You cannot modify events scheduled from an integrated third party scheduler in Avaya Video Conferencing Manager, except to add an MCU to a call or to change settings of the scheduled devices.
4. Click **Apply Changes**.

To delete a scheduled conference, click the event entry, , and **Delete Schedule**.

NOTE If Avaya Video Conferencing Manager is integrated with a third party scheduler, you cannot delete a call scheduled through that application.

Using Cascading MCUs

Use cascading MCUs to connect calls between two groups of participants. Each groups' communication is channeled through one MCU, and the MCUs pass the bundled communication between each other, greatly reducing the bandwidth needed for the groups to communicate with each other.

Consider the following example: Eight participants on a network in Japan want to conference with a group of seven participants on a network in Europe. You schedule the 15 participants in a conference along with two MCUs, one that serves the users in Japan, and one that serves the users in Europe. You then drag one of the MCUs (which becomes subservient) and drop it onto the icon for the other (which becomes the master). For this example to work, the MCUs need to know to which participants to connect. You do this by giving the devices affinity to an MCU.

NOTE If you created a PIN to use for the call when adding one or more MCUs, the same PIN is used for all cascaded MCUs.

Assign MCU affinity to a device from the **Devices** page or the **Device details** page of a device. Refer to MCU Affinity.

NOTE If you integrated a third party scheduling application, users cannot schedule a cascading MCU call from that application.

Use cascading MCUs in calls scheduled from third party scheduling applications by editing the call details from the **Events** page in Avaya Video Conferencing Manager. If you update a call scheduled from a third party scheduling application by adding cascading MCUs from the **Events** page, Avaya Video Conferencing Manager sends an email to the meeting organizer describing the changes, provided you allow sending email notifications to meeting organizers. For more information about allowing email notifications to be sent to meeting organizers, refer to Mail Integration Settings.

Viewing a Call in Progress

1. From Avaya Video Conferencing Manager Dashboard, do one of the following:
   - Under **Calls**, click **Currently in progress**.
   - Click to access the **Events** page. In the **Display** list, select **Calls in progress**.
2. Click a call, , and **Add or remove participants**.

   Each participant in the call appears with a series of icons and, for LifeSize, LG, and Avaya video systems, a snapshot from its camera. Mouse over the icons to learn what each does. With these icons you can do the following:
   - View a calendar of this device's future conferences.
   - Hang up or reconnect to the call. You can also hang up a call from the **Events** page by clicking the call, , and **Hang up call**.
   - Open call statistics.

     You can also view call statistics during a call from the following:
     - The **Devices** page by clicking a device in a call, , **Events**, and **Show call statistics**.
     - The **Events** page by clicking a call in progress, , and **Show call statistics**.
   - Open a call statistics report.
   - Mute the device.
   - Enable or disable the Do Not Disturb feature on the device (LifeSize, Avaya, and LG devices only).
   - Control the volume on the device (LifeSize, Avaya, and LG devices only).

On Demand Conferences in LifeSize Bridge

An on demand conference is a virtual conference hosted by LifeSize Bridge. On demand conferences are not scheduled in advance; do not have a scheduled start time; and are always live. If requested ports are available when the first participant attempts to join, the on demand conference begins.

NOTE On demand conferences created in Avaya Video Conferencing Manager appear in the LifeSize Bridge Utility also.

Managing All On Demand Conferences

1. Click on the navigation bar to access the **Devices** page.
2. In **Actions**, select **On demand conferences** and then click **Submit**.
3. A list of all on demand conferences appears.
4. Use the following tools to manage on demand conferences:

	Adds a new on demand conference. From the **Add new conference** dialog box, click **Show details** to configure additional conference settings.
	Shows the **Modify conference** dialog box for you to edit the on demand conference.
	Sets affinity of the on demand conference to a LifeSize Bridge. With affinity set to a LifeSize Bridge, the on demand conference is available to the LifeSize Bridge when you schedule a conference from the **Events** page.
	Adds the on demand conference to a group. When an on demand conference resides in a group, video system users can select the on demand conference through the corporate directory. Read more at Managing Device Groups.
	With a third party scheduler only: Registers the on demand conference with a mailbox resource.
	Deletes the on demand conference.

5. Select **Publish to directory** to make the conference available to the corporate directory.

NOTE If a scheduled conference uses an on demand conference's ID, you cannot change the affinity or delete the on demand conference.

Managing On Demand Conferences for a LifeSize Bridge

1. From the **Devices** page, select the LifeSize Bridge entry and click .
2. Point to **Configuration** and then click **On demand conferences**.

   On demand conferences with affinity set to the LifeSize Bridge appear.
3. *With a third party scheduler only*: Click the on demand conference entry and .

   The **Register with mailbox** dialog box appears.
4. Enter the mailbox resource you created for the conference and click **Register**.

   The yellow envelope icon changes from to .

Port Use

The number of ports Avaya Video Conferencing Manager reserves for a call hosted by LifeSize Bridge depends on the scheduling method and the conference type.

Port Use	Third Party Scheduler through Email	Avaya Video Conferencing Manager Events page
Reserve number of ports; do not allow additional ports.	Use the LifeSize Bridge email ID.	Leave **Conference ID** blank or choose a conference ID that is not for an on demand conference.
Reserve number of ports; specify number of additional ports.	Use the LifeSize Bridge email ID and specify the overbooking information in Avaya Video Conferencing Manager Administrator. Read more about overbooking at LifeSize Bridge Settings.	Leave **Conference ID** blank or choose a conference ID that is not for an on demand conference. To specify the number of reserved ports when you schedule the call, click and **Other settings**. From **Reserved ports**, choose the number of ports.
Allow flexible number of ports.	Use an on demand conference email ID.	Use an on demand conference email ID.

If you schedule a conference through a third party scheduler and include mail IDs for both a LifeSize Bridge and an on demand conference, Avaya Video Conferencing Manager uses the on demand conference.

Scheduling Template Applications and Comparisons

You can schedule the application of a template to a device, and make the template application recurrent. Alternatively, you can schedule comparisons of templates to the settings of a managed device or devices. Avaya Video Conferencing Manager generates a report of the differences between the template and the settings on the devices and sends it to the email address or addresses you have set up as alert destinations either during installation or in the Avaya Video Conferencing Manager Administrator Email Settings page. You can also make these comparisons recurrent.

Complete the following steps to schedule template actions:

1. Click to access the **Events** page.
2. In **Actions**, choose **Schedule Template** and then click **Submit**.
3. Enter the details for the template action.
   a. Enter a name for the action.
   b. Enter a start and end date and time.
   c. Select the **Make**, **Model** and **Version**. If you select **common** for **Model**, the action only affects the settings that the devices share with the template.
   d. Select the devices to which you want to apply or compare to the template.
   e. In **Template name**, select the template.
   f. In **Job Type**, select **Compare** or **Apply**.
   g. Click **Recurrence** to set up a regularly occurring template action.

   NOTE In an installation that uses ADAM for user authentication, you cannot schedule template events to recur beyond six months.

   h. Click **Schedule**.

      The event appears on the **Events** page.

Checking for Template Application Errors

Errors during the application of a template do not abort the process but are instead collected and noted in the log. Follow these steps to check for errors during a template application:

1. Access the **Templates** page.
2. In **Actions**, select **View logs** and click **Submit**.

   Failed parameters identifies parameters that were not updated correctly during the template application.

Scheduling a Device Software Upgrade

To schedule the application of one or more software upgrade packages to your devices, follow these steps:

1. Click to access the **Events** page.
2. In **Actions**, choose **Schedule Upgrade**.

NOTE You can also schedule an upgrade from the **Devices** page. Refer to Device Management Overview.

3. Enter a name for the upgrade, the start and end time for the upgrade, and identify the device or devices you want to upgrade.

NOTE In an installation that uses ADAM for user authentication, you cannot schedule upgrades beyond six months.

4. Choose a **Make** and **Model** of the device you want to upgrade.
5. In **Select devices**, select the individual devices.
6. In **Packages**, choose the package you wish to apply.
7. To upgrade a device that requires a registration key, enter the key in **Register Key**.
8. Click **Schedule** to schedule the upgrade or click **Apply Now** to start the upgrade immediately. If you choose **Schedule**, the event appears on the **Events** page as a scheduled event.

NOTE To delete a scheduled upgrade: in the **Display** list, select **All scheduled upgrades**, click the event, , and **Delete**.

Viewing Upgrade Schedules

You can view upgrade schedules by choosing **Scheduled Upgrades** in the **Display** list.

Troubleshooting Partially Successful Upgrades

If the status of a completed upgrade is **Partial success**, the event includes more than one device and only some of the devices upgraded successfully. Double-click the event to view the status of the upgrade for each device and identify which devices failed to upgrade.

Scheduling Offline Time for a Device

You can take a managed device (excluding gatekeepers and gateways) offline for a specified period of time so that Avaya Video Conferencing Manager users (and those using an integrated third party scheduler) cannot use the device in any scheduled events or manage the device in Avaya Video Conferencing Manager during that time period. This may be useful, for example, when you need to perform maintenance on a device for an extended period of time or isolate a device for dedicated use by a particular group of users.

If the device is scheduled to participate in another event during the offline time period, Avaya Video Conferencing Manager does the following:

- Deletes the scheduled event (if the event depends on the device) or modifies the scheduled event by deleting the device from the event.
- Removes the entire subconference from the call if the event is a scheduled call in which the device is the host of a cascaded subconference or the only participant in a subconference.
- Sends the meeting organizer an email indicating that the device has been removed from the call if the call was scheduled through a third party scheduling application.

Follow these steps to take a managed device offline:

1. Click to access the **Events** page.
2. In **Actions**, click **Schedule device offline** and then click **Submit**.

   The **Schedule Offline for device** dialog box appears.

   NOTE You can also access this dialog box from the **Devices** page: click a managed device, , **Events**, and **Take device offline**.

3. Enter the following information for the event:
   a. Name the event. This name identifies the event when it is listed on the **Events** page.
   b. Ensure that **Selected device** shows the IP address and name of the device that you wish to take offline.
   c. Select the date and time period to take the device offline.
   d. Click **Schedule**.
   e. If the device is already a participant in another scheduled event for that time period, Avaya Video Conferencing Manager prompts you to review the list of conflicting events. Click **Yes** to review the list. The **Events** page lists the conflicting events. To clear the conflicts, you can modify the events by clicking an event entry, , and **Edit Details**.
4. When you are finished viewing or modifying the conflicting events, click **Confirm** at the bottom of the **Events** page to delete or modify the conflicting events and create the offline event. The device offline event appears on the **Events** page as a scheduled event.

Scheduling Conferences in Microsoft Outlook

If you integrated Microsoft Exchange Server, Microsoft Outlook users in your organization can use a Microsoft Outlook meeting request to schedule conferences.

Meetings scheduled in Microsoft Outlook with managed audio or video systems appear as scheduled calls in Avaya Video Conferencing Manager on the **Events** page. The icon appears in the **Type** column on the **Events** page to indicate an event that is scheduled from Microsoft Outlook. Calls scheduled through Avaya Video Conferencing Manager also appear as events in Microsoft Outlook, thus preventing double booking.

When you schedule an upgrade or template comparison for a managed device in Avaya Video Conferencing Manager, that information is shared with Microsoft Outlook and the device becomes unavailable for scheduling other events.

If none of the devices that the meeting organizer invites to the call is capable of hosting the call, Avaya Video Conferencing Manager automatically adds an available MCU to the schedule and includes the device in the email confirmation that it sends to the meeting organizer.

Cascading MCUs are not available through Microsoft Outlook. If a meeting organizer in Microsoft Outlook includes more participating devices than the host device can connect to, or selects more than one MCU to participate in a call, Avaya Video Conferencing Manager automatically includes only one MCU and makes the selection based on the MCU affinity of the participating devices, if assigned, or the MCU with the greatest number of ports. You can modify a meeting scheduled in Avaya Video Conferencing Manager from Microsoft Outlook to include cascading MCUs only from the Avaya Video Conferencing Manager **Schedule Call** dialog box.

By default, Avaya Video Conferencing Manager automatically places a call scheduled through Microsoft Outlook. If a call fails, Avaya Video Conferencing Manager sends an error email to the meeting organizer indicating that the call failed to launch. To enable the meeting organizer to convert the call to one that is placed manually by the participants, you must enable the feature described in Specifying a Preferred Method of Participation.

NOTE Changes made in Avaya Video Conferencing Manager (such as change of MCU, bandwidth, or type of call) to a meeting scheduled through Microsoft Outlook are overwritten by a meeting update that is subsequently sent from Microsoft Outlook.

Scheduling a Conference

1. Create a meeting request in Microsoft Outlook.
2. Add invitees to the request, including the mailboxes for the audio or video systems as required attendees.

NOTE Depending on how your administrator configured Avaya Video Conferencing Manager, you may need to add the video or voice devices as separate invitees or just the conference rooms in which the devices reside. Read more at Task 4: Choose a deployment option.

If a PIN is required for the call and Avaya Video Conferencing Manager is configured to automatically generate a PIN for calls scheduled with an MCU from Microsoft Outlook, Avaya Video Conferencing Manager sends the PIN to the meeting organizer in the confirmation email when the call is scheduled. You can modify the PIN only from Avaya Video Conferencing Manager. Avaya Video Conferencing Manager sends an email to the meeting organizer indicating the new PIN. For more information about configuring Avaya Video Conferencing Manager to automatically generate a PIN for calls scheduled from Microsoft Outlook, refer to Microsoft Exchange Server Settings.

Optional: Selecting an MCU

Add an MCU to the meeting request in the same manner that you add other invitees. Only one MCU is allowed in a call scheduled from Microsoft Outlook. If you choose more than one, Avaya Video Conferencing Manager selects an MCU for you and notifies you of the selection in the confirmation email that it sends when you schedule the call.

Optional: Selecting an on demand conference

Add an on demand conference to the meeting request in the same manner that you add other invitees. If you invite a LifeSize Bridge and an on demand conference, Avaya Video Conferencing Manager uses the on demand conference settings.

Optional: Selecting a Video Conference Recorder

Add the video conference recorder invitee designated for this purpose by your administrator. Avaya Video Conferencing Manager automatically selects which video conference recorder to add to the call.

3. Send the meeting request. Avaya Video Conferencing Manager sends an email confirmation regarding the success or failure of the scheduling request. Devices with scheduling conflicts are excluded from the meeting and are noted in the confirmation email.

Updating a Meeting Request

Observe the following rules if you need to update a meeting request:

- **Webmail for Microsoft Outlook 2003**. Do not delete all devices from a meeting originally scheduled through Microsoft Outlook. Doing so does not delete the scheduled call in Avaya Video Conferencing Manager. Cancel the meeting instead of deleting all the participating devices if your intent is to cancel the meeting.
- **Microsoft Outlook 2007 and 2010**. Do not forward a meeting request to devices. Instead, add new devices to the meeting and send the update to all participants. If you forward a meeting request as a means to add devices to the scheduled call, Avaya Video Conferencing Manager includes only the new devices in the scheduled call and removes all other devices.
- **Webmail for Microsoft Outlook 2007 and 2010**. When adding or deleting participants to a scheduled call, send the meeting update to all participants when prompted. The default option sends the update only to affected participants, which results in Avaya Video Conferencing Manager deleting the original conference participants from the scheduled call.

Specifying a Preferred Method of Participation

If you integrated Microsoft Exchange Server, you can allow participants in video calls scheduled in Avaya Video Conferencing Manager through Microsoft Outlook to specify an external video communications device through which they can be reached. By default, this feature is disabled. Consider enabling this feature if the following conditions exist in your environment:

- Invitees to video meetings in your organization are mobile but have access to video systems.
- You wish to allow invitees to video meetings who are external to your organization to include their video communications devices as scheduled participants in calls scheduled through Avaya Video Conferencing Manager.

NOTE Support for specifying a preferred device is available only for video devices.

Enabling this feature also allows meeting organizers to convert a call from one that is placed automatically by Avaya Video Conferencing Manager to one that participants place manually.

To enable this feature, select **Enable participants to select a preferred method of participation** on the **Microsoft Exchange Settings** page in Avaya Video Conferencing Manager Administrator. Refer to Microsoft Exchange Server Settings.

Avaya recommends that you use this feature in a test environment before deploying it in your organization. Enabling this feature allows a meeting invitee to add an external device to Avaya Video Conferencing Manager's database without having a user account in Avaya Video Conferencing Manager. Avaya Video Conferencing Manager does not check the validity of the IP address of an external device that is added to a call through this mechanism.

CAUTION When the list of scheduled devices changes due to a reply from a human invitee to the email messages generated by this feature, all human invitees receive an email indicating the change.

When this feature is enabled and a meeting organizer schedules a video call in Avaya Video Conferencing Manager through a meeting invitation in Microsoft Outlook, Avaya Video Conferencing Manager sends a confirmation email to all participants. The email includes the conference details: the date and start time of the call, the call reservation type, and the IP addresses of the video devices that are scheduled to participate in the call. The email also includes instructions and commands that recipients can use in a reply to the email to do the following:

- Convert a call from one that is placed automatically by Avaya Video Conferencing Manager to one that is placed manually by meeting participants. Only the meeting organizer can reply to the confirmation email with the command `reservation-request` in the body of the reply. By default, Avaya Video Conferencing Manager automatically places a call scheduled through Microsoft Outlook unless it receives this command from the meeting organizer.
- Convert a call from one that is placed manually by meeting participants to one that is placed automatically by Avaya Video Conferencing Manager. Only a meeting organizer can reply to the confirmation email with the command `video-call` in the body of the reply.
- Specify the IP address of an external video communications device through which the invitee wishes to participate in the scheduled call. A meeting invitee can reply to the confirmation email with the command `call@`*IPaddress*. Avaya Video Conferencing Manager adds the device to the scheduled call and notifies the meeting organizer and all other invitees of the change. If Avaya Video Conferencing Manager has no database entry for the device, it adds the device and its IP address to its database as an external device. If the device is already a scheduled participant in the call or a managed device, Avaya Video Conferencing Manager ignores the command. For more information about external devices, refer to Managing External Devices.
- Remove an external device that an invitee added to the call with the `call@`*IPaddress* command. A meeting invitee can reply to the confirmation email with the `busy` command to remove a device that the invitee added to the call in a previous reply to the confirmation email. Avaya Video Conferencing Manager removes the external device from the scheduled call and sends an email to the meeting organizer and all other invitees of the change.

The confirmation email sent from Avaya Video Conferencing Manager to participants who are not managed devices indicates the available commands and usage to the invitees. The following rules must be observed by invitees who wish to reply:

- The confirmation email includes a conference identifier in the body of the message. Invitees who reply must include this identifier in the reply.
- The reply must be plain text. Other text formats are not supported.

Avaya Video Conferencing Manager returns an error or ignores the reply in these scenarios:

- The syntax is incorrect. The sender must reply to the original confirmation (not to the error email) with the proper syntax.
- The call is in progress.
- The user does not have permission to execute the command. Avaya Video Conferencing Manager accepts the `reservation-request` and `video-call` commands from the meeting organizer only and ignores a reply that includes either of these commands if the reply is from any other invitee.

The emails that Avaya Video Conferencing Manager sends to the meeting organizer and to invitees are available on the **Microsoft Exchange Settings** page in Avaya Video Conferencing Manager Administrator in the **Email Customization** section. The email identifiers are **Exchange - Schedule created successfully - message to organizer (1)** and **Exchange - Schedule created successfully - message to Invitees (1)**. Refer to Microsoft Exchange Server Settings.

Scheduling Conferences in Google Calendar

If you integrated Google Apps, Google Apps Calendar users in your organization can schedule video and voice conferences with a Google Apps Calendar event invitation. The icon appears in the **Type** column on the **Events** page to indicate an event that is scheduled from Google Apps Calendar. Calls scheduled through Avaya Video Conferencing Manager also appear as events in Google Apps Calendar for each resource, preventing double booking.

When you schedule an upgrade or template comparison for a managed device in Avaya Video Conferencing Manager, that information is shared with Google Apps Calendar, and the device becomes unavailable for scheduling other events.

If none of the devices that the meeting organizer invites to the call is capable of hosting the call, Avaya Video Conferencing Manager automatically adds an available MCU to the schedule and includes the device in the email confirmation that it sends to the event organizer.

Cascading MCUs are not available through Google Apps Calendar. If an event organizer in Google Apps Calendar includes more participating devices than the host device can connect to, or selects more than one MCU to participate in a call, Avaya Video Conferencing Manager automatically includes only one MCU and makes the selection based on the MCU affinity of the participating devices, if assigned, or the MCU with the greatest number of ports. You can modify an event scheduled in Avaya Video Conferencing Manager from Google Apps Calendar to include cascading MCUs only from the Avaya Video Conferencing Manager **Schedule Call** dialog box.

By default, Avaya Video Conferencing Manager automatically places a call scheduled through Google Apps Calendar. If a call fails, Avaya Video Conferencing Manager sends an error email to the event organizer indicating that the call failed to launch.

NOTE Changes made in Avaya Video Conferencing Manager (such as change of MCU, bandwidth, or type of call) to a meeting scheduled through Google Apps Calendar are overwritten by a meeting update that is subsequently sent from Google Apps Calendar.

Scheduling a Conference

1. Log in to your Google Apps Calendar account.
2. Create a new event and edit its details, or open an existing event.
3. Click the **Check guest and resource availability** link. Video communications devices or the conference rooms that are associated with them appear as resources in a list below the **Where** section of the page. Depending on how you configured Avaya Video Conferencing Manager, you may need to add the video or voice communications devices as separate resources or just the conference rooms in which the devices reside. Refer to Configuring Google Apps for Use with Avaya Video Conferencing Manager.
4. Double-click a resource to add it to the event.
5. Add attendees and click **Save changes**.

   Add an MCU to the meeting request in the same manner that you add other resources. Only one MCU is allowed in a call scheduled from Google Apps Calendar. If you choose more than one, Avaya Video Conferencing Manager selects an MCU for you and notifies you of the selection in the confirmation email that it sends when you schedule the call. If a PIN is required for the call and Avaya Video Conferencing Manager is configured to automatically generate a PIN, Avaya Video Conferencing Manager sends the PIN to the event organizer in the confirmation email when the call is scheduled. You can modify the PIN only in Avaya Video Conferencing Manager. If modified, Avaya Video Conferencing Manager sends an email to the event organizer indicating the new PIN. For more information about automatically generating a PIN, refer to Google Apps Settings.

   Add an on demand conference to the meeting request in the same manner that you add other invitees. If you invite a LifeSize Bridge and an on demand conference, Avaya Video Conferencing Manager uses the on demand conference settings.

   Add the video conference recorder resource designated for this purpose by your administrator. Avaya Video Conferencing Manager automatically selects which video conference recorder to include in the call.
6. Save and send the event.

   Emails from the resources appear in the inbox of the Avaya Video Conferencing Manager user in Google Apps Gmail. The calendars of these resources appear as blocked in the Google Apps calendar of the Avaya Video Conferencing Manager user. Avaya Video Conferencing Manager sends an email confirmation to the event organizer regarding the success or failure of the scheduling request. Devices with scheduling conflicts are excluded from the meeting and are noted in the confirmation email.

Creating Repeating Events in Google Apps Calendar

Avaya Video Conferencing Manager accepts repeating events scheduled from Google Apps Calendar provided the event has an end date. Avaya Video Conferencing Manager does not support repeating events that specify the **Never** option for the end date.

Modifying an Event in Google Apps Calendar

If you make any of the following modifications to an event in Google Apps Calendar, Avaya Video Conferencing Manager updates the event on the **Events** page in Avaya Video Conferencing Manager provided the resources invited to the event are free for the proposed time:

- Add or remove a participant or resource.

  CAUTION Do not add or remove a resource using the links below **Guests** in an event.

- Change the event time.
- Modify the subject or description of the event.

Cancelling an Event in Google Apps Calendar

If you use Google Apps Calendar to cancel an event that was scheduled in Avaya Video Conferencing Manager from Google Apps Calendar, be sure to select the option to delete and notify guests when deleting the event. Avaya Video Conferencing Manager deletes the event from its **Events** page.

Section 4: Generating Reports

Avaya Video Conferencing Manager provides the following options for generating reports:

Periodic	Shows data between specified dates. You can specify a range of dates, or choose a particular day, week, month, or year. Periodic reports include: • Call statistics show the distribution of calls for the specified duration. • Maximum port utilization shows the number of ports used by LifeSize Bridge for the specified duration. • Maximum traversal by LifeSize Transit shows the call count through LifeSize Transit for the specified duration. • Firewall NAT call statistics show the call count and minutes for calls that traversed the firewall or whose IP addresses were translated across networks (NAT). Error statistics (distribution of errors over a specific period; error types appear in different colors). Device specific reports list activity for a group of devices on the network.
Inventory	Shows information about current devices. Types of inventory reports include hardware audit (listing of hardware types and capabilities) and serial number audit (where devices are located).
Summary	Shows information based on calendar month and year. Types of summary reports include yearly managers summary reports by month or by week.
License Audit	Shows licensed devices by model.
Location Audit	Shows devices by location.
ROI	Shows device utilization by IP address and by model.
Codec	Shows transmit, receive, and resolution reports on communications systems.
Conference Audit	Contains conference-specific statistics.
User Audit	Shows user-specific usage details.
Billing	Shows the estimated cost of calls over a specified date range by device or by location.
Diagnostic	Represents diagnostic information related to audio and video jitter and packet loss by location or device.
Complete CDR Data	Lists the first 100 call detail records (CDRs) for video communications devices. Exported data includes all CDRs.

NOTE CDR data is also available for LifeSize Multipoint if the MCU is registered to LifeSize Gatekeeper in Avaya Video Conferencing Manager.

You can generate data and graphical reports that you can export to PDF or CSV formats. You can also subscribe to a recurring report that is sent to the email address associated with your user account.

Follow these steps to view reports:

1. Click on the navigation bar to access the **Reports** page.
2. Use the hierarchy listing on the left to expand the view.
3. Click the report you want to view.
4. Set the report options and click **OK**.

NOTE Select the **Subscribe details** option to set a generation time and the frequency at which the reports are sent to your email. You must have an email address associated with your user account.

5. By default, the report appears as a graph (when available). To view the report as a table, select **Table** in the **View As** options at the top of the **Reports** page.
6. Optionally, to export a report in either PDF or CSV format, select the format from **Export As** and then click **Submit**. The CSV format is available for selection in **Export As** only for report data that appears in a table.

Device Utilization

By default for reporting, the call count does not include individual participants in the call. For example, Avaya Video Conferencing Manager counts a video conference with six participants as one call, not six. If this call lasts 10 minutes, regardless of the number of participating devices, Avaya Video Conferencing Manager reports the time used as 10 minutes, not 60. Avaya Video Conferencing Manager produces a CDR for the entire conference instead of adding the CDRs of the constituent legs.

To instruct Avaya Video Conferencing Manager to count each constituent leg as a call and count its time used as part of the total time used, select the **Double count** checkbox when generating reports. The following reports are affected by this option:

- Periodic reports: Call statistics
- Summary reports: Manager summary (includes traffic protocol, traffic success, traffic failure, and error summary)
- Location audit report

In conferences involving multiple managed devices, the aggregate CDR begins when the first device joins, and ends when the last device exits the conference. Affected reports include:

- Periodic reports: Device specific reports
- Summary reports: Manager summary (includes device summary and device call minutes) and Device utilization reports
- ROI reports: Device utilization report, Device specific utilization report, and Individual utilization and ROI reports (included in the Manager summary)

Viewing System Audits

The **System Audit** page shows actions performed in Avaya Video Conferencing Manager:

- by a selected user
- automatically by the Avaya Video Conferencing Manager server during a server session or by a logged in user during a server session
- on a managed device

NOTE Actions performed on managed LifeSize Desktop installations are viewable in the **Operation history** window on the LifeSize Desktop page.

Access the **System Audit** page by clicking on the navigation bar. The default view shows the first 100 entries. To view the next or additional 100 entries, use the page numbers or **Go to page** box at the bottom of the page. Use the **Search** box at the top of the page to search for information on the current page.

Double-click an entry; or click an entry, , and **View details** to view details of the action.

Click any column heading to sort all entries by ascending or descending order based on the information in that column.

You can choose how audit entries appear on the **System Audit** page in the following ways:

Columns	Click to select additional columns of information or hide columns.
Browse	Click to browse actions. Choose one of the following audit types: • **User Audit**: View all actions performed by a Avaya Video Conferencing Manager user. • **Session Audit**: View all actions performed automatically by the Avaya Video Conferencing Manager server between the start and stop time of the server and, optionally, by a specific logged in user during the selected session. • **Device Audit**: View all actions performed on a managed device by make and model. Expand the folders that appear below the audit type and select a value. Click **Show all** to clear a view and show all actions.
Refresh	Click to refresh entries on the current **System Audit** page.
Search	Search for actions by one or more criteria. Click to open the **Search** window. Select the search criteria, and then select values from lists, if available, for a selected attribute. Scroll to the bottom of the **Search** window and click **Search**. Click **Show all** to clear a search and show all entries.

Exporting System Audit Entries

Use **Export** on the **System Audit** page to export all entries as either a CSV or PDF file. Use the Shift+click or Ctrl+click keys to select a subset of all entries to export. Click one of the selected entries, , and **Export selected - CSV file format** or **Export selected - PDF file format**.

Section 5: Administering Avaya Video Conferencing Manager

Avaya Video Conferencing Manager Administrator is a web-based tool for administrators. Click on the navigation bar to access the tool.

Application Settings	Configure settings for location, device discovery, system logs, device polling frequency, time-out interval for automatic logout, and HTTP proxy settings. Read more at Application Settings.
Alarms	Enable or disable alarms and specify alarm severity. Read more at Alarms Configuration.
Database	Back up and restore the database. Read more at Database Management.
Billing	Configure settings for estimating call costs. Read more at Billing Information.
Conferences	Configure settings for monitoring calls. Read more at Conference Settings.
Email	Configure settings for email alerts and messages. Read more at Email Settings.
Conference Alert Thresholds	Modify alert threshold settings for audio and video in calls. Read more at Conference Alert Threshold Settings.
LDAP	Modify LDAP configuration settings. Read more at LDAP Settings.
Device License Uploads	Upload a list of device license keys for LifeSize devices.
Diagnostics	View version information, port status, and the status of services used by the application. Read more at Diagnostics.
SNMP Traps	Enable or disable forwarding of SNMP traps. Read more at Northbound Settings.
LifeSize Bridge	Associate an email address to reserve extra ports for conferences hosted by LifeSize Bridge and scheduled through Microsoft Exchange. Including the email address as an attendee reserves extra ports on LifeSize Bridge. Read more at LifeSize Bridge Settings.
Roles	Create additional roles to customize user access to features and associated tasks. Read more at Role Management Settings.
Mail Integration	Configure settings for integration with the third party scheduling application that you chose during installation of Avaya Video Conferencing Manager. Read more at Mail Integration Settings.

Application Settings

Click **Application Settings** to modify the following Avaya Video Conferencing Manager configuration settings. Click **Save** for your changes to take effect.

Setting	Description
Location Settings	Configures the country, state, and IP address for the Avaya Video Conferencing Manager server.
Device Discovery	When **DHCP Scan** (network scan) is **ON**, Avaya Video Conferencing Manager automatically scans for supported devices in subnets in which it currently manages devices. For example, if Avaya Video Conferencing Manager manages a device with the IP address 10.95.11.121, DHCP scan, if enabled, scans for supported devices in the IP address range 10.95.11.0 through 10.95.11.255. By default, **DHCP Scan** is **OFF**. Consider enabling DHCP scan when devices do not retain their DHCP assigned address for long periods of time or if devices in the specified IP address range are added to or removed from the network frequently.
System Logs	Avaya recommends that you change this setting only when directed by Avaya Technical Services to troubleshoot an issue with Avaya Video Conferencing Manager. The default setting is **ERROR**. Changing this setting to **DEBUG** or **WARNING** may produce large log files.
Monitoring	Sets the time interval after which Avaya Video Conferencing Manager polls the status of managed devices. The default is 5 minutes.
Automated Logout	Specifies the length of time, in minutes, after which Avaya Video Conferencing Manager automatically logs off a user due to inactivity. The default is 30 minutes. Enter 0 to disable this feature.
Proxy Address	Defines the address of the HTTP proxy server between Avaya Video Conferencing Manager and LifeSize Transit.
Proxy Bypass List	Lists addresses that bypass the proxy server. Examples include: `http://10.*` and `LDAP://*`.
Proxy Username and **Password**	Username and password for the proxy server.

Alarms Configuration

To determine the status and severity of available alarms, select a type from **Category**, and select an alarm ID from the **Alarms** box. The alert message for the alarm appears below the **Alarms** box, along with its **Status** (**ON** or **OFF**) and severity (**INFO**, **LOW**, **MEDIUM**, or **HIGH**).

To assist you in identifying alarms that you may wish to turn off, the category and the alarm ID appear in the email notification that is sent when an alarm is triggered. Alarms by Category lists all alarm IDs and the message, default status, and default severity associated with each.

If you change the status or severity of an alarm, click **Save** to save your changes. You must also restart the Avaya Video Conferencing Manager Service for the changes to take effect: from the machine on which Avaya Video Conferencing Manager is installed, open Windows **Services**.

Database Management

Click **Database Management** to back up the PostgreSQL database and associated files. The current **Database Edition** appears at the top of the page.

Backing up the Avaya Video Conferencing Manager Database

1. Click **Back up Database** to create a PostgreSQL database backup.

   A file download dialog box shows the date-stamped backup file.

2. Click **Save**.

Restoring the Avaya Video Conferencing Manager Database from a Backup

1. Click **Browse** and locate the proper backup file.
2. Click **Restore Database**.

CAUTION	Restoring a database backup file overwrites current data and cannot be undone.

Billing Information

Avaya Video Conferencing Manager uses billing information to estimate the cost of calls placed with your audio and video communications devices. Click **Billing Information** to update the cost per KB by location.

To add or update an entry, select the **Country**, **State**, and **Call Type**, and enter the **Cost Per KB**. The currency you choose is used for all entries.

NOTE	Ensure that the country and state are also configured on the devices that you wish to include in the billing reports. No data appears in billing reports if the country and state are not set on the devices and in Avaya Video Conferencing Manager Administrator.

Click **Add/Update** to save your changes before you add or update another entry.

To delete an entry, select the **Country**, **State** (if applicable), and **Call Type**, and click **Delete**.

Conference Settings

Click **Conference Settings** to modify the following configuration settings for calls and conferences. Click **Save** for your changes to take effect.

Setting	Description
Monitor call statistics	Select this checkbox to compile statistics for managed calls.
Show snapshots with call details	Select this checkbox to show a snapshot from each participant in a call when viewing a call in progress from the **Events** page. NOTE: Snapshots are available for managed LifeSize, LG, and Avaya devices only.
Collect call statistics	Select this checkbox to show a statistics graph from each participant in a call when viewing a call in progress or completed calls from the **Events** page.
Call Termination Alert Interval	Enter the time, in minutes, before the end of a call at which time Avaya Video Conferencing Manager will send an alarm and email to the administrator regarding a call's termination. The default is 15 minutes.
Call Statistics Monitoring Interval	Enter the time interval to define the frequency at which Avaya Video Conferencing Manager polls current call statistics. NOTE: The default setting of 3 minutes may cause high CPU usage for the `LSCService.exe` process during calls and slow response to tasks performed with the user interface. Depending on the volume of calls and the CPU requirements of other applications running on the server, you may wish to disable **Monitor call statistics** or increase the time interval.
Call Retry Attempts	Enter the number of times a conference will retry a failed call. The default is 1.

Email Settings

Click **Email Settings** to modify the following configuration settings for email alerts and messages. Click **Save** for your changes to take effect.

Setting	Description
SMTP Server	Enter the address of the SMTP server Avaya Video Conferencing Manager uses to send emails about alarms. For Microsoft Exchange enabled users, use the email server address you specified for the Microsoft Exchange Server IP in the **Mail Integration Settings** page.
Email Address	Enter the addresses of recipients of email alerts. You can enter multiple addresses separated by commas.
From Address	Enter the address to use for the source of the email alerts.

Conference Alert Threshold Settings

Click **Conference Threshold Settings** to modify the following alert threshold settings for audio and video in calls. When Avaya Video Conferencing Manager detects figures above these thresholds, it sends an alert to the email addresses listed as recipients on the **Email Settings** page.

Setting		Value
Audio	**Transmit Jitter**	Enter a value between 1 and 1000. The default is 40.
	Receive Jitter	Enter a value between 1 and 1000. The default is 40.
	Transmit Packet Loss %	Enter a value between 1 and 100. The default is 5.
	Receive Packet Loss %	Enter a value between 1 and 100. The default is 5.
Video	**Transmit Jitter**	Enter a value between 1 and 1000. The default is 100.
	Receive Jitter	Enter a value between 1 and 1000. The default is 100.
	Transmit Packet Loss %	Enter a value between 1 and 100. The default is 5.
	Receive Packet Loss %	Enter a value between 1 and 100. The default is 5.
	Transmit F/S	Enter a value between 1 and 60. The default is 7.
	Receiver F/S	Enter a value between 1 and 60. The default is 7.

LDAP Settings

Click **LDAP Settings** to modify the following LDAP configuration settings. Click **Save** for your changes to take effect.

Setting		Description
LDAP Settings	**LDAP Server IP Address**	Specifies the IP address of the ADAM server.
	Port	You cannot modify **Port**.
	Domain Suffix for the LDAP Directory	Specifies the domain suffix for the ADAM directory.
User Authentication	**Configure for LDAP** -OR- **Configure for Active Directory**	The available option depends on whether you chose ADAM or Active Directory for user authentication when you installed Avaya Video Conferencing Manager.
	Username **Password**	If you chose Active Directory, you can change the username and password that you specified during installation. The new account must be a domain account with the ability to search the Active Directory. If you chose ADAM, you can change only the account password (to update the password in Avaya Video Conferencing Manager if you changed it in ADAM).

Diagnostics

Click **Diagnostics** to view version information, port status, and the status of services used by the application.

To start or stop services listed under **Service Name**, access the machine on which Avaya Video Conferencing Manager is installed and open Windows **Services**.

Port Status lists the status of ports required by the application. When the Avaya Video Conferencing Manager service is stopped, none of these ports should be in use. If one or more are in use, some other application or service is using those ports and may interfere with the proper execution of the application.

Northbound Settings

Click **Northbound Settings** to enable or disable forwarding of SNMP traps (alarms) and configure trap destinations to which Avaya Video Conferencing Manager forwards traps from all managed video and voice communications devices. By default, SNMP trap forwarding is enabled.

If you configure trap destinations in Avaya Video Conferencing Manager Administrator, Avaya Video Conferencing Manager forwards traps from all managed video and voice communication devices to these destinations. To specify trap destinations for a single device, use the **Northbound** tab on the **Device details** page of the device. Refer to Forwarding SNMP Traps with Northbound Settings.

Clear the **Enable Avaya Video Conferencing Manager Northbound Settings** checkbox and click **Save** to disable SNMP trap forwarding.

NOTE Clearing this checkbox disables SNMP trap forwarding from all managed video and voice devices. This also removes access to the **Northbound** tab on the **Device details** page of all devices and disables forwarding traps to any device-specific destinations specified on the **Northbound** tab. If you disable trap forwarding, refresh your browser before accessing the **Device details** page for a managed video or voice device.

Add a trap destination for forwarding SNMP traps for all managed video and voice devices by defining the following, and clicking **Add** and **Save**:

IP Address	Address to which Avaya Video Conferencing Manager forwards SNMP traps from managed video and voice communication devices.
Port	Destination port on the IP address to which Avaya Video Conferencing Manager forwards the SNMP trap.
Username	Used for authentication on the specified IP address (not to exceed 40 characters).
Password	Used for authentication on the specified IP address (not to exceed 40 characters).

To remove a trap destination, click its IP address and click **Delete**.

LifeSize Bridge Settings

Use Avaya Video Conferencing Manager Administrator to associate an email address with extra ports for conferences hosted by LifeSize Bridge and scheduled through Microsoft Exchange. Including the email address as an attendee in a scheduled conference instructs Avaya Video Conferencing Manager to reserve extra ports on LifeSize Bridge for that conference.

Configure overbooking by setting **Overbooking email** and **Overbooking number**.

NOTE An email address associated with extra ports can be used only with LifeSize Bridge.

Role Management Settings

A user role identifies the tasks that users assigned to the role are authorized to perform in Avaya Video Conferencing Manager. Click **Role Management Settings** to do the following:

- *Administrators only*: Create, modify, or delete a custom user role.
- View the page-level tasks that all roles are authorized to perform. To view the list of tasks that the administrator, engineer, and operator roles are authorized to perform on pages and devices, refer to User Role Access.

NOTE You cannot edit or delete the three predefined roles in Avaya Video Conferencing Manager: Administrator, Engineer, and Operator.

Read more about user accounts and role assignments at Managing User Accounts.

Creating a Role

1. Click **Create New Role**.
2. Enter a name and a description for the role.
3. In the **Settings** section, each tab corresponds to a page in Avaya Video Conferencing Manager and the associated tasks that users assigned to the role can be authorized to perform on that page. Click each tab to expand the category and select the tasks that you wish to assign to this role.

NOTE The **Reset** button clears all selections for the role.

4. Click **Save**.

5. Custom roles created in Avaya Video Conferencing Manager Administrator are not automatically authorized to perform tasks on devices. To assign tasks that can be performed on devices to a custom role, refer to Managing Device Permissions Groups for Custom Roles.

Modifying a Role

1. In **Select Role**, click the custom role you wish to modify. You cannot modify or delete the Administrator, Engineer, or Operator roles.
2. If desired, revise the name and description for the role.
3. In **Settings**, click each tab to expand the category and select the tasks that you wish to assign to this role.
4. Click **Save Updates**.

Deleting a Role

You can delete a role only if the role is not assigned to a user account. For more information about modifying user accounts, including modifying a user's role assignment and deleting a user account, refer to Managing User Accounts.

Mail Integration Settings

Enable or disable and modify the configuration settings for the integration of a third party scheduling application from the **Mail Integration Settings** page.

If you change any of these settings, click **Save** below **Recorder email** for your changes to take effect. You must also restart the Avaya Video Conferencing Manager service for the changes to take effect. To start or stop the Avaya Video Conferencing Manager service, access the machine on which Avaya Video Conferencing Manager is installed and open Windows **Services**.

In the **Email Customization** section on this page, you can customize the email messages that Avaya Video Conferencing Manager automatically generates and sends to Microsoft Outlook or Google Apps users. Use **Email Identifier** to select a message. The subject and text of the selected message appear in **Email Subject** and **Email Body**. You can also choose whether Avaya Video Conferencing Manager sends any of these messages by selecting or clearing the **Send this email** checkbox that appears with each message.

CAUTION Avoid changing any line of text that includes the $ symbol. At minimum, do not delete the $ symbol.

If you change email customization settings, click **Save** below **Email Body** for your changes to take effect. Use the **Reset** button to return the messages to default values.

Microsoft Exchange Server Settings

If you chose Active Directory for user authentication when you installed Avaya Video Conferencing Manager, you can modify the following Microsoft Exchange Server settings from the **Mail Integration Settings** page:

Setting	Description
Enable Mail integration	Enable this feature and select the version of Microsoft Exchange Server used in the integration.
Require HTTPS Access	Select this checkbox to require secure HTTP.
Autogenerate PIN for calls scheduled through Microsoft Exchange	Select this checkbox to automatically generate a PIN for a conference call when a meeting organizer adds an MCU to a meeting request.
Enable device management through email	Select this checkbox to enable administrators to manage devices with email commands. For more information about available commands, refer to Managing a Device Through Email.
Enable participants to select a preferred method of participation	Select this checkbox if you wish to enable meeting invitees to a video conference that is scheduled through Microsoft Outlook to add an external video device to a call. By default, this feature is disabled. Enabling this feature also enables the meeting organizer to specify whether to place the call automatically by Avaya Video Conferencing Manager or place the call manually by the meeting participants. CAUTION: Enabling this feature allows a meeting invitee to add an external device to Avaya Video Conferencing Manager's database without having a Avaya Video Conferencing Manager user account. Read more at Specifying a Preferred Method of Participation.
Maximum number of days for schedules to be allowed within	Set the maximum scheduling timeframe.
Microsoft Exchange Server IP	Enter the IP address of the Microsoft Exchange Server.
Microsoft Exchange Server Domain	Enter the Microsoft Exchange server domain name.
Microsoft Exchange User	Enter the username of the Avaya Video Conferencing Manager email account in Microsoft Exchange. This is the account Avaya Video Conferencing Manager monitors to provide scheduling integration with Microsoft Exchange Server.
Avaya Video Conferencing Manager Email	Enter the email address of the account Avaya Video Conferencing Manager monitors to provide scheduling integration with Microsoft Exchange Server. Read more at Avaya Video Conferencing Manager email address.
Password	Enter a password for the Avaya Video Conferencing Manager email account.
Recorder Email	Enter the email address of the resource mailbox that you created for managed video conference recorders.

NOTE The email identifiers **Exchange - Schedule created successfully - message to organizer (1)** and **Exchange - Schedule created successfully - message to Invitees (1)** are sent only when the **Enable participants to select a preferred method of participation** checkbox is selected. Refer to Specifying a Preferred Method of Participation.

Google Apps Settings

If you chose Microsoft ADAM for user authentication when you installed Avaya Video Conferencing Manager, you can modify the following Google Apps Gmail and Google Apps Calendar settings from the **Mail Integration Settings** page:

Setting	Description
Enable Mail integration	If you enable this feature, click **Gmail**.
Autogenerate PIN for calls scheduled through Gmail	Select this box to automatically generate a PIN for a conference call when an event organizer adds an MCU to a meeting request.
Maximum number of days for schedules to be allowed within	Set the maximum scheduling timeframe.
Avaya Video Conferencing Manager Email	Enter the email address of the account Avaya Video Conferencing Manager monitors to provide scheduling integration with Google Apps Gmail and Google Apps Calendar.
Password	Enter a password for the Avaya Video Conferencing Manager email account.
Recorder resource name	If you are managing video conference recorders in Avaya Video Conferencing Manager, enter the resource name of the resource mailbox that you created for managed video conference recorders.

Section 6: Reference

User Role Access

The following tables describe the tasks that the administrator, engineer, and operator user roles are authorized to perform in Avaya Video Conferencing Manager.

Tasks can be performed either on a page or on a device. Tables that identify page-level tasks include the word **Page** in the table title. These tasks appear in the **Role Management Settings** page in Avaya Video Conferencing Manager Administrator. For information about creating custom roles, refer to Role Management Settings.

The last table identifies device-level tasks. These tasks appear in the **Manage IT group** window as part of device groups features that are accessible on the **Devices** page. These tasks can be assigned to custom roles. Refer to Managing Device Groups.

NOTE The following tables do not include tasks in Avaya Video Conferencing Manager Administrator. Only administrators can access Avaya Video Conferencing Manager Administrator.

Alarms Page

Task	Administrator	Engineer	Operator
View details	Yes	Yes	Yes
Acknowledge alarm	Yes	Yes	No
Own alarms	Yes	Yes	No
Acknowledge alarms with resolution	Yes	Yes	No
Forward alarms	Yes	Yes	No
Assign alarms	Yes	No	No
Unacknowledge alarm	Yes	Yes	No
Export all alarms to CSV	Yes	No	No
Export all alarms to PDF	Yes	No	No
Export selected - CSV file format	Yes	No	No
Export selected - PDF	Yes	No	No

Devices Page

Task	Administrator	Engineer	Operator
View list of devices	Yes	Yes	Yes
Discover devices	Yes	Yes	No
Manage devices	Yes	Yes	No
Delete device	Yes	Yes	No
Scan network	Yes	Yes	No
Add external device	Yes	Yes	No
Export view as PDF	Yes	Yes	No
Manage device groups	Yes	Yes	No
Manage permissions on devices	Yes	No	No
Infrastructure management	Yes	No	No

Events Page

Task	Administrator	Engineer	Operator
View list of events	Yes	Yes	Yes
View details	Yes	Yes	Yes
Schedule calls	Yes	Yes	Yes
Redial completed calls	Yes	Yes	Yes
Show call statistics	Yes	Yes	Yes
Drop call	Yes	Yes	Yes
Add or remove participants in call	Yes	Yes	Yes
Edit calls	Yes	Yes	Yes
Delete calls	Yes	Yes	Yes
Schedule device upgrades	Yes	Yes	No
Delete scheduled upgrades	Yes	Yes	No
Edit device upgrades	Yes	Yes	No
View system calendar	Yes	Yes	No
Schedule device offline	Yes	No	No
Delete device offline	Yes	No	No
Edit device offline	Yes	No	No
Schedule template events	Yes	No	No

Task	Administrator	Engineer	Operator
Delete template events	Yes	No	No
Edit template events	Yes	No	No

Reports Page

Task	Administrator	Engineer	Operator
View reports	Yes	Yes	Yes
Export reports as PDF	Yes	Yes	No
Subscribe to reports	Yes	Yes	No

Templates Page

Task	Administrator	Engineer	Operator
View templates	Yes	No	No
Apply template	Yes	No	No
Edit template	Yes	No	No
Compare template	Yes	No	No
Delete template	Yes	No	No
Create template	Yes	No	No
Create template from device	Yes	No	No
Back up device	Yes	No	No
Restore device	Yes	No	No
View logs	Yes	No	No

Packages Page

Task	Administrator	Engineer	Operator
View packages	Yes	Yes	Yes
Upload packages	Yes	Yes	No
Delete packages	Yes	Yes	No

Password Page

Task	Administrator	Engineer	Operator
View password details	Yes	No	No
Edit SNMP v1 or SNMP v2	Yes	No	No
Add SNMP v3 user	Yes	No	No
Modify SNMP v3 user	Yes	No	No
Delete SNMP v3 user	Yes	No	No
Add for other protocols	Yes	No	No

User Management Page

Task	Administrator	Engineer	Operator
View list of users	Yes	Yes	Yes
Modify self details	Yes	Yes (ADAM installations only)	Yes (ADAM installations only)
Import or add new user	Yes	No	No

License Manager Page

Task	Administrator	Engineer	Operator
View license details	Yes	No	No
Enter license key	Yes	No	No
Enter unlock key	Yes	No	No

System Audit Page

Task	Administrator	Engineer	Operator
View details	Yes	Yes	Yes
Export all to CSV	Yes	No	No
Export all to PDF	Yes	No	No
Export selected - CSV	Yes	No	No
Export selected - PDF	Yes	No	No

LifeSize Desktop Page

Task	Administrator	Engineer	Operator
View details	Yes	Yes	Yes
Manage LifeSize Desktop	Yes	Yes	No
Unmanage	Yes	Yes	No
Delete LifeSize Desktop	Yes	Yes	No
Change password	Yes	Yes	No
Create template from the device	Yes	Yes	No
Apply template	Yes	Yes	No
View operation history	Yes	Yes	No
Deactivate license	Yes	Yes	No
Activate license	Yes	Yes	No
Manage groups	Yes	Yes	No
LifeSize Desktop provisioning	Yes	No	No
Export all LifeSize Desktop instances as CSV	Yes	Yes	No
Export all LifeSize Desktop instances as PDF	Yes	Yes	No

Help Page

Task	Administrator	Engineer	Operator
Access Help for using Avaya Video Conferencing Manager	Yes	Yes	Yes

Device-level Permissions

Task	Administrator	Engineer	Operator
View devices	Yes	Yes	Yes
View details	Yes	Yes	Yes
Launch browser interface	Yes	Yes	No
Update password	Yes	Yes	No
Change password	Yes	Yes	No
View alarms	Yes	Yes	No
Schedule upgrade	Yes	Yes	No

Task	Administrator	Engineer	Operator
Reboot device	Yes	Yes	No
Take device offline	Yes	Yes	No
Register with mailbox	Yes	Yes	No
Set the MCU affinity	Yes	Yes	No
Register with gatekeeper	Yes	Yes	No
Update the license key	Yes	Yes	No
Send message	Yes	Yes	No
View snapshots	Yes	Yes	No
Apply settings	Yes	Yes	No
Create template	Yes	Yes	No
Refresh device	Yes	Yes	No
View calendar	Yes	Yes	No
Recorder affinity	Yes	Yes	No
Join conference	Yes	Yes	No
Discover registered devices	Yes	Yes	No
Bring device online	Yes	Yes	No
Show call statistics	Yes	Yes	No

Alarms by Category

conference

Alarm ID	Description	Default Status	Default Severity
ID_ABNORMAL_CALL_TERMINATION	Abnormal termination of the conference.	ON	HIGH
ID_ADHOC_CONFERENCE_AT_RISK	Adhoc conference 1 with meeting ID 2 is at risk. Minimum required ports : 3	ON	MEDIUM
ID_ADHOC_LIVE_CONFERENCE_AT_RISK	Adhoc Live conference 1 with meeting ID 2 is at risk. Minimum required ports : 3	ON	HIGH
ID_CONF_DEV_BUSY_AT_SCHEDULED_TIME	One or more devices added to this conference are busy for the scheduled time.	ON	HIGH
ID_CONF_EXTERNAL_EP_UNAVAILABLE	One of the external participants in the conference 1 is not available.	ON	HIGH
ID_CONF_FAILED_EMPTY_DEV_LIST	Failed to launch conference 1. Empty device list.	ON	HIGH
ID_CONF_LAUNCH_FAIL_INSUFFICIENT_DEV	Failed to launch conference 1. Not enough devices are running.	ON	HIGH
ID_CONF_LAUNCH_FAILED_NO_DEV	Failed to launch conference 1. No managed devices found.	ON	HIGH
ID_CONF_SAVE_FAILED	Failed to save conference 1. No managed devices were found.	ON	HIGH
ID_CONF_TERMINATION_PENDING	Conference 1 is pending termination.	ON	HIGH
ID_COULD_NOT_RECORD_THE_CONFERENCE	Conference 2 could not be recorded.	ON	HIGH
ID_DEL_CONF_FAILED_DB_ERROR	Failed to delete conference 1 from the conference table; a database error occurred.	ON	MEDIUM
ID_DEL_CONF_FAILED_NO_MATCH_FOUND	Failed to delete the conference 1 from the conference table. No matching conference was found.	ON	MEDIUM
ID_DESKTOP_REPORT_PROBLEM	The LifeSize Desktop instance 1 has reported a problem.	ON	HIGH
ID_DEVICE_LICENSE_HAS_EXPIRED	1 devices are approaching renewal.	ON	HIGH

Alarm ID	Description	Default Status	Default Severity
ID_FAILED_UPDATE_CONF_STATUS_TO_TERMINATED	Failed to update the status of the conference 1 to terminated.	ON	MEDIUM
ID_INVALID_RECORDING_PIN	Conference 2 could not be recorded.	ON	HIGH
ID_NO_FREE_SLOTS_IN_RECORDER	Conference 2 could not be recorded.	ON	HIGH
ID_PERIODIC_CDR_FAILURE	Failed to fetch CDR.	ON	MEDIUM
ID_RECORDER_DOWN	Conference 2 could not be recorded.	ON	HIGH
ID_RECORDING_FAILED_UNREGISTERED_DEVICES	Recorder could not record a conference containing MCU.	ON	HIGH
ID_UNABLE_TO_MAKE_CALLS	Unable to make a call to 1 from 2.	ON	HIGH
ID_UNABLE_TO_MAKE_CALLS_NO_SERVICE_PREFIX	Unable to make a call to 1 from 2. MCU does not have a valid service prefix.	ON	HIGH

general

Alarm ID	Description	Default Status	Default Severity
ID_LINK_DOWN	Link down.	ON	MEDIUM
ID_AUTH_FAIL	Authentication failure.	ON	MEDIUM

LDAP

Alarm ID	Description	Default Status	Default Severity
ID_LDAP_CONNECT_ERROR	Unable to connect to the server.	ON	HIGH

LifeSize

Alarm ID	Description	Default Status	Default Severity
ID_TS_CALL_CAPACITYREACHED	Maximum call capacity reached for Transit Server 1	ON	MEDIUM
ID_TS_DATABASE_PROBLEM	Database error for Transit Server 1	ON	HIGH
ID_TS_LICENSE_EXPIRED	Expired license for Transit Server 1	ON	HIGH

Alarm ID	Description	Default Status	Default Severity
ID_TS_TUNNEL_DOWN	Tunnel is down for Transit Server 1	ON	MEDIUM
ID_PROVISION_FAILED	Provisioning failed for 1	ON	MEDIUM
ID_TS_CALL_REACHING_MAXCAPACITY	Approaching maximum call capacity for Transit Server 1	ON	MEDIUM
ID_SYSTEM_HEAT_STATUS_OVERHEATED	System is overheated.	ON	HIGH
ID_SYSTEM_HEAT_STATUS_WARNING	System heat status is abnormal.	ON	MEDIUM

Avaya Video Conferencing Manager

Alarm ID	Description	Default Status	Default Severity
ID_CALL_STATS_ALARM	A call statistics threshold violation has occurred.	ON	HIGH
ID_DEV_LICENSE_NOT_SUPP	Device license is not supported.	ON	HIGH
ID_DEV_STATUS_INAPPROPRIATE_FOR_DEL	Device deletion failed. Device status is not appropriate for deletion.	ON	HIGH
ID_DEVICE_DOWN	The device is not running.	ON	HIGH
ID_DEVICE_DOWN_BETWEEN	The device was not running.	ON	HIGH
ID_DIR_CREATE_FAIL	Failed to create the required directory structure.	ON	MEDIUM
ID_EXCHANGE_CONTROL_INTEGRATION_DOWN	Integration with Microsoft Exchange Server is not operational.	ON	HIGH
ID_FAILED_DEV_REBOOT	Failed to reboot the device.	ON	HIGH
ID_LOW_LICENSE_COUNT	Available licenses remaining are less than 15% of the total licenses.	ON	MEDIUM
ID_MODIFY_CONF_DB_ERROR	Failed to modify conference 1. Database error.	ON	MEDIUM
ID_MODIFY_CONF_FAIL_NO_MGMD_DEV	Failed to modify conference 1. No managed devices found.	ON	MEDIUM
ID_MODIFY_CONF_NO_MATCH	Failed to modify conference 1. No matching conference found.	ON	MEDIUM
ID_NO_MORE_LICENSES	No licenses left.	ON	HIGH
ID_SERVER_CONNECT_ERROR	Unable to connect to the server.	ON	MEDIUM
ID_UNKNOWN_ERROR	An unknown error has occurred.	ON	MEDIUM

Alarm ID	Description	Default Status	Default Severity
ID_UPDATE_PWD_ON_DEV_FAILED	Failed to update the password on the device.	ON	MEDIUM
ID_USER_FAILED_TO_LOGIN	User 1 failed to log in.	ON	MEDIUM
ID_USER_FAILED_TO_LOGIN_LDAP_ERROR	User 1 failed to log in, LDAP server error.	ON	MEDIUM

Polycom

Alarm ID	Description	Default Status	Default Severity
ID_POLYCOM_AUTH_FAILURE	Authentication failure.	ON	MEDIUM
ID_POLYCOM_BATTERY_LOW	Low battery.	ON	MEDIUM
ID_POLYCOM_CALL_FAILED	Call failed.	ON	MEDIUM
ID_POLYCOM_JITTER_EXCESSIVE	Jitter is excessive.	ON	HIGH
ID_POLYCOM_LATENCY_EXSS	Latency is excessive.	ON	HIGH
ID_POLYCOM_LINE_DOWN	Line down.	ON	MEDIUM
ID_POLYCOM_LOGIN_FAILED	Login failed.	ON	MEDIUM
ID_POLYCOM_MAIN_CAM_DOWN	Main camera is not running.	ON	MEDIUM
ID_POLYCOM_MIC_CHANGE	Microphone change.	ON	MEDIUM
ID_POLYCOM_PERCENT_PACK_LOSS_EXSS	Percentage of packet loss is excessive.	ON	HIGH

software upgrade

Alarm ID	Description	Default Status	Default Severity
ID_SW_UPGRADE_CANCELLED_NOW	The upgrade could not occur since the device is currently not reachable.	ON	HIGH
ID_SW_UPGRADE_FAILED	The software upgrade failed.	ON	HIGH
ID_SW_UPGRADE_FAILED_LOGIN	The software upgrade failed because of a login failure.	ON	HIGH
ID_SW_UPGRADE_FAILED_PACKAGE_NOT_FOUND	The software upgrade failed because the file 1 does not exist.	ON	HIGH

Tandberg

Alarm ID	Description	Default Status	Default Severity
ID_TANDBERG_GENERAL_ERR	callLastError has been set with a new message, indicating a codec problem. Check SNMP MIB for more info.	ON	MEDIUM
ID_TANDBERG_IP_AUTH_FAIL	IP authentication failure.	ON	MEDIUM
ID_TANDBERG_LOW_BATTERY	Low battery.	ON	MEDIUM
ID_TANDBERG_LOW_SPEEDING	Down speeding.	ON	MEDIUM

Section 7: Troubleshooting

If your Avaya Video Conferencing Manager installation or upgrade fails, or you cannot access the user interface after performing an installation or upgrade, use the information in this section to resolve the issue. For all other issues, or if the issue persists, contact Technical Services for assistance.

NOTE To avoid installation errors, disable security software (including Windows Firewall) before running the Avaya Video Conferencing Manager installer. After installation, you may re-enable security software.

Exporting Page Views

At the top of most pages in Avaya Video Conferencing Manager is an option to export the current view as a PDF document. This feature is useful for troubleshooting when you are working with support representatives.

Starting and Stopping Avaya Video Conferencing Manager

To stop the Avaya Video Conferencing Manager Server in the Windows **Services** window on the machine on which Avaya Video Conferencing Manager is installed, use the **Start** option to restart the service. Using the **Restart** option produces an error.

Maintenance with Microsoft Exchange Server Integration

Once integrated, Avaya Video Conferencing Manager will not run correctly if Microsoft Exchange Server 2007 goes down or is offline. If you must disable Microsoft Exchange 2007 Server, disable Microsoft Exchange integration in Avaya Video Conferencing Manager Administrator first. No conferences scheduled through Microsoft Outlook will be lost.

Firewall Issues

Avaya Video Conferencing Manager must be able to ping devices on the network. Ensure your firewall is not blocking ping requests. A device’s status changes to **Unreachable** if Avaya Video Conferencing Manager cannot ping it.

Installation Errors

The Avaya Video Conferencing Manager installer returns an error message and quits if any of the following conditions exist:

- An incompatible version of OpenSSL exists. Read more at OpenSSL version.
- Data folders from a previous, removed PostgreSQL installation exist and the Avaya Video Conferencing Manager installer cannot delete them. Delete the folders and then run the Avaya Video Conferencing Manager installer.
- During a new installation of Avaya Video Conferencing Manager, an installation of PostgreSQL already exists. Remove the existing PostgreSQL installation and then run the Avaya Video Conferencing Manager installer.
- During a new installation or upgrade of Avaya Video Conferencing Manager, ADAM or AD LDS does not exist on the server. Install ADAM or AD LDS as indicated in Installing Microsoft ADAM or AD LDS.
- Free disk space is insufficient. Make available at least 500 MB of free disk space on the server and then run the Avaya Video Conferencing Manager installer.
- The upgrade process does not support the current Avaya Video Conferencing Manager installation. Contact Avaya Technical Services for assistance.

During an installation of Avaya Video Conferencing Manager, the following status message may appear.

```
Could not access VBScript runtime for custom action <name of custom action>
```

The Windows Scripting Host (WSH) is needed to run a VBScript custom action during the installation, but the WSH is not installed on the target machine. Follow the instructions for downloading and installing Microsoft Windows Script 5.6 at:

```
http://www.microsoft.com/downloads/details.aspx?familyid=C717D943-7E4B-4622-86EB-95A22B832CAA&displaylang=en
```

Web Sites in IIS Function Improperly After an Upgrade

During an upgrade, the Avaya Video Conferencing Manager installer changes the ASP.NET version of all web sites installed in IIS to v2.0. Other web sites installed in IIS that are not running in their own application pools and that rely on an earlier version of Microsoft .NET Framework may function improperly after the upgrade. To work around this issue, do the following after performing the upgrade:

1. Open the IIS Manager. Click **Start->Programs->Administrative Tools->IIS Manager**.
2. Expand **Web Sites->Default Web Site**.
3. For each web application under **Default Web Site**, right-click the application and select **Properties**.
4. Click the **ASP.NET** tab. Ensure that the version is set to the appropriate Framework version for the application. For Avaya Video Conferencing Manager, the version is 2.0.

Device Status Not Updating

Device status may fail to update dynamically if other services or applications are listening on ports 161 or 162. Ensure that only Avaya Video Conferencing Manager is listening on these ports. Read more at Ports.

Login Issues

If the Avaya Video Conferencing Manager launch page does not appear when you attempt to access the user interface, do the following on the computer on which Avaya Video Conferencing Manager is installed:

Access Windows **Services** and ensure that the **IIS Admin** service is started.

If you installed Avaya Video Conferencing Manager by upgrading from a previous version, reset the IIS service: **Start->Run** and enter `iisreset`.

Access Avaya Video Conferencing Manager Administrator and do the following:

1. Click **Diagnostics** and ensure that the status of all services listed in the **Service Name** column is `Running`.
2. Click **LDAP Settings**. Ensure that the IP address that you selected for the ADAM server during installation is correct. If it is not, select the correct IP address and click **Save**.

If you are still unable to connect to the web server, you may need to reassign the server certificate to correct the problem:

1. From **Start->Run**, enter `inetmgr`.
2. Expand the tree to expose the **Default Web Site** node.
3. Right-click the **Default Web Site** node and click **Properties**.
4. Click the **Directory Security** tab and click **Server Certificate**.
5. Click **Next**.
6. Select the **Assign an existing certificate** option and click **Next**.
7. Select the certificate displayed in the selection box and click **Next**.
8. Select the default SSL port and click **Next**.
9. Click **Next** and click **Finish**.
10. From **Start->Run**, enter `inetmgr`.

    The IIS web server restarts and you should be able to access the Avaya Video Conferencing Manager web page using HTTPS.

© 2011 Avaya Inc.
All Rights Reserved.

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types
Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (see "Third Party Components" for more information).

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:
http://support.avaya.com/Copyright

Preventing toll fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention
If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:
http://support.avaya.com
Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks
Avaya and Aura are trademarks of Avaya, Inc.
Avaya is a registered trademark of Avaya Inc.
Avaya Aura is a registered trademark of Avaya Inc.
All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support Web site:
http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Patent Notice
For patents covering LifeSize® products, refer to http://www.lifesize.com/support/legal.